(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－260121
（P2000－260121A）
(43)公開日　平成12年９月22日(2000.9.22)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10	301	Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４ ３０１Ｚ

審査請求　未請求　請求項の数９　ＯＬ　（全 25 頁）

(21)出願番号　特願平11－58890

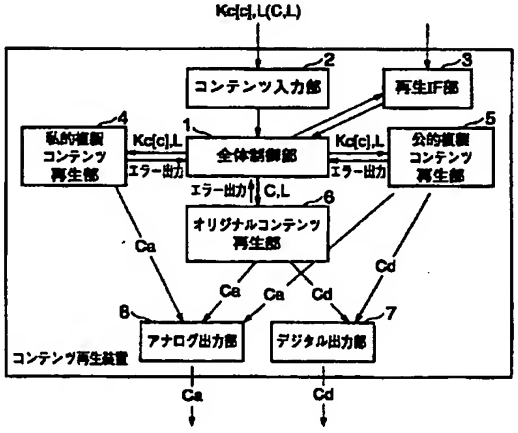
(22)出願日　平成11年３月５日(1999.3.5)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　情報再生装置および情報記録装置

(57)【要約】
【課題】正当な経路で複製されたコンテンツ（公的複製コンテンツ）が、正当な権限なく複製されたコンテンツよりも有利な形態で流通可能となる。
【解決手段】本発明の情報再生装置は、コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報に基づき該コンテンツ情報を再生する情報再生装置において、暗号化されたコンテンツ情報を前記ライセンス情報の内容に基づき公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する判別手段と、この判別手段で私的複製コンテンツ情報と判別されたコンテンツ情報は、公的複製コンテンツ情報よりも厳しい制限で再生する再生手段とを具備する。



1

【特許請求の範囲】

【請求項１】　コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報に基づき該コンテンツ情報を再生する情報再生装置において、
暗号化されたコンテンツ情報を前記ライセンス情報の内容に基づき公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する判別手段と、
この判別手段で私的複製コンテンツ情報と判別されたコンテンツ情報は、公的複製コンテンツ情報よりも厳しい制限で再生する再生手段と、
を具備したことを特徴とする情報再生装置。

【請求項２】　前記ライセンス情報に含まれる公的複製であることを検証するための検証情報に基づき、公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別することを特徴とする請求項１記載の情報再生装置。

【請求項３】　前記ライセンス情報に含まれる前記コンテンツ情報の利用条件は、私的複製コンテンツ情報の方が公的複製コンテンツ情報よりも制限されていることを特徴とする請求項１記載の情報再生装置。

【請求項４】　前記コンテンツ情報に付加されたライセンス情報は、該コンテンツ情報の記録されている記録媒体の識別子に依存する情報に基づき作成された鍵情報で暗号化および復号化されることを特徴とする請求項１記載の情報再生装置。

【請求項５】　前記判別手段は、前記ライセンス情報の内容に基づき前記コンテンツ情報がオリジナルコンテンツ情報であるかを判別するものであり、オリジナルコンテンツ情報と判別されたときは、該コンテンツ情報を無制限に再生する第２の再生手段をさらに具備したことを特徴とする請求項１記載の情報再生装置。

【請求項６】　コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、
入力されたコンテンツ情報の種別を判別する判別手段と、
この判別手段で判別された種別および前記記録媒体の識別子に依存する情報に基づき前記ライセンス情報を作成する作成手段と、
この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段と、
を具備したことを特徴とする情報記録装置。

【請求項７】　コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、
入力されたコンテンツ情報の種別を判別する判別手段と、
この判別手段で判別された種別および前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき前記ライセンス情報を作成する作成手段と、
この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段と、
を具備したことを特徴とする情報記録装置。

【請求項８】　前記入力されたコンテンツ情報は、アナログ信号であることを特徴とする請求項６または請求項７記載の情報記録装置。

【請求項９】　コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、
前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき公的複製であることを検証するための検証情報を含む前記ライセンス情報を作成する作成手段と、
この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段と、
を具備したことを特徴とする情報記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は画像や音声等のコンテンツの記録再生装置に関する。

【０００２】

【従来の技術】ＣＤプレーヤを始めとするデジタルコンテンツ再生装置は音質が綺麗なこと、長時間の使用による音質劣化が少ないことなどから、多くの利用者がある。

【０００３】しかし、コンテンツがデジタルであるが１ビットずつオリジナルを忠実に複製することによって、劣化なくコピーすることが可能となっており、実際そのような機器が販売されている。そのようなコピー機器の存在はコンテンツ利用者にとっては大きなメリットではあるが、コンテンツ供給者からはコンテンツの販売に甚大な影響を与えるために好ましくはない。このためコンテンツ供給業者は新しいデジタル機器（及びメディア）が出た際はこれにコンテンツを供給しないことで対抗している。

【０００４】だが、この状況は、新しい電子機器の普及にあたって、大きな障害となり、その利便性を殆どの人が享受できないばかりかコンテンツ供給者もビジネスチャンスを失っている。

【０００５】また一方で、私的利用のための私的複製は著作権法でも認められた権利であり、実際現在までの多くの電子機器にあっては（アナログ記録への制限など）複製方式に制限はあるが認められてきた。だが、今後デジタルでの記録が主流になると私的複製と公的複製の区別が付きにくくなると同時に私的利用の判別が難しくなる。

【０００６】なお、ここでは、私的複製とは当該ソース

の販売権を持たない人によるコピーを言い、公的複製は当該ソースに販売権を持つ人によるコピーを言う。即ち、公的複製とは従来のコンテンツ販売と同等の手段でなければ取得できないものであり、インターネット上の電子商店からの販売も含まれる。

【０００７】

【発明が解決しようとする課題】以上の問題点に鑑み、本発明は、コンテンツが公的複製であるか私的複製であるによって当該コンテンツの再生方式を切り替え、公的複製の方が私的複製よりも有利な利用形態を許すことにより、正式な販路にのっている公的複製の需要を増やし、コンテンツ供給者、コンテンツ利用者、電子機器供給者に利害にかなった情報流通機構を構築できる情報再生装置、情報記録装置および情報販売装置および情報購入装置および情報自動販売機を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明では前記の課題を解決するため、暗号化コンテンツの利用を当該暗号化コンテンツに対応するライセンス情報によって制御すると同時に、公的複製である暗号化コンテンツに対応したライセンス情報にはコンテンツ販売が許可されているコンテンツ販売サーバだけが知っている公開鍵暗号方式の秘密鍵によって署名することにより、デジタル署名の有無によって公的複製と私的複製を判別し、判別結果に基づいて当該コンテンツの再生手段を変え、公的複製の方が私的複製よりも有利な再生手段で再生できる方式を実現する。

【０００９】（１）本発明の情報再生装置は、コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報に基づき該コンテンツ情報を再生する情報再生装置において、暗号化されたコンテンツ情報を前記ライセンス情報の内容に基づき公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する判別手段と、この判別手段で私的複製コンテンツ情報と判別されたコンテンツ情報は、公的複製コンテンツ情報よりも厳しい制限で再生する再生手段とを具備する。

【００１０】また、前記ライセンス情報に含まれる公的複製であることを検証するための検証情報に基づき、公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する。

【００１１】また、前記ライセンス情報に含まれる前記コンテンツ情報の利用条件は、私的複製コンテンツ情報の方が公的複製コンテンツ情報よりも制限されている。

【００１２】また、前記コンテンツ情報に付加されたライセンス情報は、該コンテンツ情報の記録されている記録媒体の識別子に依存する情報に基づき作成された鍵情報で暗号化および復号化される。

【００１３】また、前記判別手段は、前記ライセンス情報の内容に基づき前記コンテンツ情報がオリジナルコンテンツ情報であるかを判別するものであり、オリジナルコンテンツ情報と判別されたときは、該コンテンツ情報を無制限に再生する第２の再生手段をさらに具備する。

【００１４】本発明の情報再生装置によれば、私的複製コンテンツと公的複製コンテンツやオリジナルコンテンツとの再生方法に構造上の差異を設け、私的複製を認めながら私的利用の拡大を防ぎ、著作権及びコンテンツ供給業者を保護している。

【００１５】また、コンテンツを別の記録媒体に不正に移す、即ちコピーした場合、ライセンス情報は、記録媒体に依存したものであるため、例えば、ライセンス情報が復号できなくなり、この結果としてコンテンツの復号ができくなるため、私的複製あっても公的複製であっても、コピーのためにはライセンス情報を作り直さなければならなく、それができるのは（例えば関数ｆを知る）正当な記録装置だけであるためコピーの回数の制限などが確実に行なえることから不正利用を防止することができる。

【００１６】（２）本発明の情報記録装置は、コンテンツ情報（暗号化されている場合と暗号化されていない場合とがある）と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報（暗号化されたコンテンツ情報の復号鍵を含む場合もある）とを記録媒体に記録する情報記録装置において、入力されたコンテンツ情報の種別を判別する判別手段と、この判別手段で判別された種別および前記記録媒体の識別子に依存する情報に基づき前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段とを具備している。

【００１７】本発明の情報記録装置は、コンテンツ情報（暗号化されている場合と暗号化されていない場合とがある）と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報（暗号化されたコンテンツ情報の復号鍵を含む場合もある）とを記録媒体に記録する情報記録装置において、入力されたコンテンツ情報の種別を判別する判別手段と、この判別手段で判別された種別および前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段とを具備している。

【００１８】また、上記情報記録装置において、記録するコンテンツ情報は、アナログ信号に制限されてもよい。

【００１９】本発明の情報記録装置によれば、コンテンツの種類を判別して、ソースのコンテンツよりも厳しい制限でしか複製できないような環境を提供することにより、正式な販路に載った公的複製コンテンツと私的複製

コンテンツを差別化し、公的複製コンテンツの価値を相対的に上げることにより、公的複製コンテンツの販路の拡大に寄与する。

【００２０】また、コンテンツを別メディアに不正に移す、即ちコピーした場合、ライセンス情報は、メディアに依存したものであるため、例えば、ライセンス情報が復号できなくなり、この結果としてコンテンツの復号ができくなるため、私的複製あっても公的複製であっても、コピーのためにはライセンス情報を作り直さなければならなく、それができるのは（例えば関数ｆを知る）正当な記録装置だけであるためコピーの回数の制限などが確実に行なえることから不正利用を防止することができる。

【００２１】また、記録されるソースコンテンツをアナログのみに限定することで、デジタルコンテンツを記録する際、複製を重ねる毎にコンテンツの質的劣化を引き起こすことができ、複製の抑止力となると同時に公的複製コンテンツの価値を相対的に上げ、公的複製コンテンツの販売市場を確保することがより確実にできる。

【００２２】（３）本発明の情報記録装置は、コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき公的複製であることを検証するための検証情報を含む前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段とを具備している。

【００２３】この情報記録装置は、特に、公的複製コンテンツを販売購入するためのコンテンツ販売装置、コンテンツ購入装置に用いることができる。

【００２４】また、ライセンス情報は、記録媒体に依存したライセンス情報を作成するため、私的複製であっても公的複製であっても、コピーのためにはライセンス情報を作り直さなければならなく、それができるのは（例えば関数ｆを知る）正当な記録装置だけであるためコピーの回数の制限などが確実に行なえることから不正利用を防止することができる。

【００２５】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照して説明する。

【００２６】まず、以下の説明で用いる用語について説明する。

【００２７】ライセンス情報は、コンテンツ自体に埋め込まれるものと、暗号化コンテンツに付加情報として関連付けられる外部情報とがある。ここで前者は電子透かしの手法でアナログレイヤで実現され、ここではアナログライセンス情報と呼ぶことにする。後者は、デジタルレイヤで実現されるので、デジタルライセンス情報と呼ぶ。さらに、両者を併せてライセンス情報という。

【００２８】本発明のコンテンツ記録再生装置に入力されるコンテンツは３種類あり、オリジナルコンテンツ、公的複製コンテンツ、私的複製コンテンツである。

【００２９】オリジナルコンテンツは自作のコンテンツか、コピーフリーで特定の利用制限がないコンテンツである。このためオリジナルコンテンツは暗号化されていないし、後述するライセンスヘッダのみのデジタルライセンス情報が付加されているものとする。

【００３０】公的複製コンテンツとは当該コンテンツの販売権を持つ者によって複製されたコンテンツをいう。公的複製コンテンツはコンテンツが暗号化されていると同時に販売権を証明するデジタル署名が付加されたデジタルライセンス情報が付けられている。

【００３１】私的複製コンテンツとは当該コンテンツの販売権を持たない者によって複製されたコンテンツをいう。私的複製コンテンツはコンテンツが暗号化されていると同時にデジタル署名が付加されていないデジタルライセンス情報が付けられている。

【００３２】次に、デジタルライセンス情報の具体的な構造について説明する。デジタルライセンス情報Ｌｏは、図１に示すようにライセンスヘッダ（ＬＨ）、コンテンツ鍵（Ｋｃ）、コンテンツ利用条件（Ｕ）、認証子（ＭＡＣ）、デジタル署名からなっている。

【００３３】ライセンスヘッダは、図３に示すようにライセンス情報の長さ、コンテンツの識別子（ＩＤ）、複製情報、コンテンツ鍵の長さからなっている固定長のデータである。ライセンス情報の長さはライセンス情報の全体長を示しており、ライセンス抽出時に利用する。複製情報は、当該コンテンツがオリジナルコンテンツか、公的複製コンテンツか、私的複製コンテンツかを区別するための情報である。コンテンツ鍵の長さはライセンス情報に含まれるコンテンツ鍵の長さを示す。

【００３４】デジタルライセンス情報中のコンテンツ利用条件Ｕは、当該デジタルライセンス情報に対応しているコンテンツの利用条件を示しており、図４に示すような構成をしている。図４において、デジタル出力フラグＦｅは「１」のとき、当該コンテンツのデジタル出力を許可し、「０」のときは許可しない。有効期限情報は当該コンテンツの有効期限を示している。同様に有効回数は当該コンテンツが利用できる回数を指定している。これらは全てシステムによって定められた固定長のデータである。

【００３５】なお、ここで示したデジタルライセンス情報はほんの一例であって、応用形態によって様々に変更される。

【００３６】認証子はデジタルライセンス情報に含まれるコンテンツ鍵やコンテンツ利用条件が正しいものであるかチェックするためのデータであって、誤り検出と改竄防止の効果を持っている。

【００３７】デジタル署名は、図６に示すように、デジタル署名ヘッダとデジタル署名とからなる。なお、デジタル署名ヘッダは、図７に示すように、デジタル署名の全体長（ビット長）と、当該デジタル署名の種類と署名検証鍵番号とからなっている。

【００３８】デジタルライセンス情報Ｌｏにはコンテンツ鍵Ｋｃが含まれているので暗号化されなくてはならない。しかし一方で、デジタルライセンス情報を全て暗号化してしまうと、複製情報を取得するだけの目的でも復号しなくてはならなくなったり、オリジナルコンテンツのように本来暗号化の必要のないものまで暗号化する必要が生じる。これを避けるため本実施形態では、図２に示すように、暗号化の範囲をコンテンツ鍵、コンテンツ利用条件、認証子の部分に限る構成を示している。図２にも示されているように、以下では、情報Ｉを鍵Ｋで暗号化したデータをＩ［Ｋ］もしくは［Ｋ］Ｉと表すことにする。また、デジタルライセンス情報およびコンテンツの暗号化には共通鍵暗号を使うことを前提としている。共通鍵暗号は暗号鍵と復号鍵とが一致している暗号方式である。以下の実施形態においては文脈上、復号鍵で暗号化したり、暗号鍵で復号したりする記述があるが、これは前記の理由により矛盾するものではない。

【００３９】暗号化デジタルライセンス情報は図２のような構造をしており、ライセンスヘッダとデジタル署名を除く部分を後に詳しく述べるライセンス鍵で暗号化する。

【００４０】次に、アナログライセンス情報に関して説明する。アナログライセンス情報は、電子透かしとしてコンテンツ自体に埋め込まれるものであって、再生されたアナログコンテンツに埋め込まれているので、暗号によるコンテンツの著作権保護が破れても尚有効である。だが一方で、コンテンツ自体に情報を埋め込むので、埋め込みに時間がかかるという欠点がある。

【００４１】そこで、本実施形態では、アナログライセンス情報として図５に示すような構造を考える。即ち、アナログライセンス情報１は、コピー回数制限情報と複製情報からなり、コピー回数制限情報は当該コンテンツのコピー回数の（無制限を含む）上限値を表わし、複製情報は図３のライセンスヘッダＬＨに含まれる複製情報と同じ情報が入る。

【００４２】（第１の実施形態）第１の実施形態では、入力されたコンテンツがオリジナルコンテンツ、私的複製コンテンツ、公的複製コンテンツであるかをライセンス情報を基に判別し、それに伴ってコンテンツの再生方式を変えるコンテンツ再生装置について説明する。

【００４３】本実施形態に係るコンテンツ再生装置の全体構成図を図８に、処理の流れを図１２のフローチャートに示している。以下、図１２のフローチャートを参照しながら図８のコンテンツ再生装置について説明する。

【００４４】まず、再生ＩＦ部３からの再生指示により、コンテンツ入力部２にコンテンツＣと暗号化デジタルライセンス情報Ｌを入力する（ステップＳ１）。これらの情報は全体制御部１に送られ、ここで暗号化デジタルライセンス情報のライセンスヘッダを参照して、当該コンテンツがオリジナルコンテンツか、私的複製コンテンツか、公的複製コンテンツかを識別し（ステップＳ２～ステップＳ４）、その識別結果に応じて、それぞれ、オリジナルコンテンツの再生処理、私的複製コンテンツの再生処理、公的複製コンテンツの再生処理を行なう（ステップＳ６～ステップＳ８）。

【００４５】これら３種類のコンテンツに該当しないものは、本発明のコンテンツ再生装置において解釈ができないコンテンツであるので、エラー出力を行ない、処理を終了する（ステップＳ５）。

【００４６】３つの種類に応じたコンテンツ毎の再生処理は図８のそれぞれの再生部において行なわれる。これらの具体的な構成と処理の流れに関しては後述するが、私的複製コンテンツ再生部４からデジタル出力部７へコンテンツが流れないような構成を取る点は重要である。即ち、私的複製コンテンツは私的利用の目的のみに再生が許可されたものであり、コンテンツの一部を切り貼りするなどの２次利用に関しては私的利用の範囲を逸脱する可能性が高く、コンテンツ供給業者としては許可し難い。本発明では、この点に鑑み、私的複製コンテンツと公的複製コンテンツやオリジナルコンテンツとの再生方法に構造上の差異を設け、私的複製を認めながら私的利用の拡大を防ぎ、著作権及びコンテンツ供給業者を保護している。

【００４７】図８のオリジナルコンテンツ再生部６の構成図を図９に、その処理の流れを図１３に示す。オリジナルコンテンツは前述したように、暗号化されていないコンテンツを言う。ライセンス情報に関しては、本実施形態においては、デジタルライセンス情報はライセンスヘッダのみ、アナログライセンス情報に関してはコピー回数を無制限で設定されているものとする。

【００４８】以下、図１３のフローチャートを参照しながら図９のオリジナルコンテンツの再生部６について説明する。

【００４９】オリジナルコンテンツは、コンテンツ入力部６ｃに入力し（ステップＳ２１）、データ解凍部６ｆでＭＰＥＧなどの圧縮形式が解凍されて（ステップＳ２２）、その結果出力されるデジタルコンテンツＣに関してＤ／Ａ変換部６ｇにてデジタル信号からアナログ信号に変換（Ｄ／Ａ変換）する（ステップＳ２３）。そして、アナログライセンス情報検出部６ｄにて、コンテンツに埋め込まれたアナログライセンス情報を検出したら（ステップＳ２４）、制御部６ａは、その中の複製情報を参照することにより、当該コンテンツがオリジナルコンテンツであるかどうかを判別する（ステップＳ２５）。もし、オリジナルコンテンツでなければその時点

でエラーを出力して終了する（ステップＳ２９）。オリジナルコンテンツであれば、デジタル出力の指示が来ている場合は（ステップＳ２６）、デジタル出力部６ｅを介してデジタル出力を（ステップＳ３０）、そうでない場合は、デジタルコンテンツＣをＤ／Ａ変換部６ｇでデジタル信号からアナログ信号に変換し、アナログ出力部６ｈを介して出力する（ステップＳ２７～ステップＳ２８）。

【００５０】図８の私的複製コンテンツ再生部４の構成図を図１０に、その処理の流れを図１４に示す。私的複製コンテンツは前述したように、暗号化されており、デジタルライセンス情報に（公的複製であることを証明する）デジタル署名がないコンテンツを言う。

【００５１】以下、図１４のフローチャートを参照しながら図１０の私的複製コンテンツ再生部４について説明する。

【００５２】私的複製コンテンツは、暗号化デジタルライセンス情報Ｌとともに、暗号コンテンツ入力部４ｂに入力する（ステップＳ３１）。これらの情報は暗号化コンテンツ復号部４ｃに送られ、ここで後に詳しく述べる処理によって暗号化デジタルライセンス情報を復号し（ステップＳ３２）、デジタルライセンス情報に含まれるコンテンツ鍵Ｋｃを用いて暗号化コンテンツを復号する。また、デジタルライセンス情報から利用条件Ｕを抽出する（ステップＳ３３～ステップＳ３５）。

【００５３】制御部４ａは、利用条件Ｕをチェックし（ステップＳ３６）、利用不可能と判定された場合はエラーを出力して終了する（ステップＳ４２）。利用可能であった場合、更に、利用条件に記載されている条件が私的複製コンテンツに許可されている範囲（上限値）を逸脱しているか否かをチェックする。ここで逸脱している場合は当該条件を上限値に設定した上でステップＳ３７へ進む。このようにすることによって、ライセンス情報の偽造などにシステムとして対応できる。

【００５４】制御部４ａは、復号されたコンテンツＣをデータ解凍部４ｄへ送り、ＭＰＥＧなどの圧縮形式を解凍し、デジタルコンテンツＣｄを出力する（ステップＳ３７）。デジタルコンテンツＣｄに対してＤ／Ａ変換部４ｅにてデジタル信号からアナログ信号に変換した後（ステップＳ３８）、アナログライセンス情報検出部４ｆはコンテンツに埋め込まれたアナログライセンス情報を検出する（ステップＳ３９）。そして、制御部４ａは、アナログライセンス情報の中の複製情報を参照することにより、当該コンテンツが私的複製コンテンツであるかどうかを判別する（ステップＳ４０）。もし、私的複製コンテンツでなければその時点でエラーを出力して終了する（ステップＳ４３）。私的複製コンテンツであれば、Ｄ／Ａ変換部４ｅでＤ／Ａ変換し、アナログ出力部４ｇを介してアナログ出力を行なう（ステップＳ４１）。なお、ここでデジタル出力の指示が来ていてもデジタル出力は行なわない。

【００５５】図８の公的複製コンテンツ再生部５の構成図を図１１に、その処理の流れを図１５に示す。公的複製コンテンツは前述したように、暗号化されており、デジタルライセンス情報に（公的複製であることを証明する）デジタル署名が付加されているコンテンツを言う。

【００５６】以下、図１５のフローチャートを参照しながら図１１の公的複製コンテンツ再生部５について説明する。

【００５７】公的複製コンテンツは、暗号コンテンツ入力部５ｂに暗号化デジタルライセンス情報とともに入力される（ステップＳ５１）。これらの情報は暗号化コンテンツ復号部５ｃに送られ、ここで後に詳しく述べる処理によって暗号化デジタルライセンス情報にデジタル署名が付加されているかを検証し、付加されている場合は、デジタル署名検証鍵を用いてデジタル署名を検証することによって公的複製であることを検証する（ステップＳ５２～ステップＳ５３）。なお、ステップＳ５２でデジタル署名が付加していなかった場合、ステップＳ５３でデジタル署名が検証できなかった場合はエラーを出力し処理を終了する（ステップＳ６４～ステップＳ６５）。

【００５８】ステップＳ５３でデジタル署名が検証できた場合は、後に詳しく述べる処理によって暗号化デジタルライセンス情報を復号し（ステップＳ５４）、デジタルライセンス情報に含まれるコンテンツ鍵Ｋｃを用いて暗号化コンテンツを復号する。また、デジタルライセンス情報から利用条件Ｕを抽出する（ステップＳ５５～ステップＳ５７）。

【００５９】制御部５ａは、利用条件をチェックし（ステップＳ５８）、利用不可能と判定された場合はエラーを出力して終了する（ステップＳ６６）。利用可能であった場合、更に、利用条件に記載されている条件が私的複製コンテンツに許可されている範囲（上限値）を逸脱しているか否かをチェックする。ここで逸脱している場合は当該条件を上限値に設定した上でステップＳ５９へ進む。このようにすることによって、ライセンス情報の偽造などにシステムとして対応できる。

【００６０】制御部５ａは、復号されたコンテンツＣをデータ解凍部５ｄへ送り、ＭＰＥＧなどの圧縮形式を解凍し、デジタルコンテンツＣｄを出力する（ステップＳ５９）。デジタルコンテンツＣｄに対してＤ／Ａ変換部５ｅでＤ／Ａ変換を行った後（ステップＳ６０）、アナログライセンス情報検出部５ｆは、コンテンツに埋め込まれたアナログライセンスを検出する。そして、制御部５ａは、アナログライセンス情報の中の複製情報を参照することにより、当該コンテンツが公的複製コンテンツであるかどうかを判別する（ステップＳ６１）。もし、公的複製コンテンツでなければその時点でエラーを出力して終了する（ステップＳ６７）。公的複製コンテンツ

であれば、デジタル出力の指示が来ている場合は（ステップＳ６２）デジタル出力部５ｉを介してデジタル出力を（ステップＳ６８）、そうでない場合はＤ／Ａ変換部５ｅでＤ／Ａ変換し、アナログ出力部５ｇを介してアナログ出力を行なう（ステップＳ６３）。

【００６１】次に、暗号化コンテンツ復号部について説明する。この構成部は、私的複製コンテンツ再生部４、公的複製コンテンツ再生部５に存在し、どちらも構成は類似している。まず、公的複製コンテンツ再生部５の暗号化コンテンツ復号部５ｃについて述べ、私的複製コンテンツ再生部４の暗号化コンテンツ復号部４ｃに関しては暗号化コンテンツ復号部５ｃとの差異のみを述べることにする。

【００６２】暗号化コンテンツ復号部５ｃの構成例を図１６に、その処理の流れを図１８に示す。以下、図１８のフローチャートを参照して暗号化コンテンツ復号部５ｃについて説明する。

【００６３】暗号化コンテンツＫｃ［C］と暗号化デジタルライセンス情報Ｌとが暗号化ライセンス復号部５ｃに入力すると（ステップＳ７１）、暗号化ライセンス復号部５ｃでは、メディアＩＤ抽出部（公的複製コンテンツ再生部５の場合は、メディアＩＤ抽出部５ｈ、私的複製コンテンツ再生部４の場合は、メディアＩＤ抽出部４ｈ）を通じて当該コンテンツの記録されていたメディアＭの識別子であるメディアＩＤを取得する（ステップＳ７２）。そのメディアＩＤを用いて、後に詳しく述べる手段により、ライセンス復号鍵ｗを作成し、復号されたデジタルライセンス情報を出力する（ステップＳ７３）。

【００６４】図１に示すデジタルライセンス情報のうち、コンテンツ鍵Ｋｃとコンテンツ利用条件Ｕから認証子を計算する（ステップＳ７５）。認証子は、例えばコンテンツ鍵とコンテンツ利用条件を連結した情報を一方向性関数の入力として出力された値とする。

【００６５】ここでの認証子の役割は、ライセンス鍵ｗが間違っているために間違ったコンテンツ復号鍵や利用条件が出力されることがないようにする誤り検出の役割である。ＭＡＣの生成は一方向性関数によって実現される。一方向性関数はハッシュ関数や暗号関数によっても実現され、出力値から入力値が推定できないような関数をいう。

【００６６】ＭＡＣ照合部１０２は、暗号化ライセンス復号部１０１からの出力から計算された認証子と、同じく暗号化ライセンス復号部１０１から出力された図１のデジタルライセンス情報にもともと含まれている認証子ＭＡＣとを照合して（ステップＳ７６）、一致すれば出力されたコンテンツ復号鍵Ｋｃは信頼できるので（ステップＳ７７）、このＫｃを用いて、コンテンツ復号部１０３にて、暗号化コンテンツを復号する（ステップＳ７８）。認証子が一致しなかった場合は、エラー出力し処理を終える（ステップＳ８１）。

【００６７】認証子を照合し、暗号化コンテンツが復号できた場合、コンテンツＣと利用条件Ｕを出力し、暗号化コンテンツ復号部の処理を終了する（ステップＳ７９）。

【００６８】次に、暗号化コンテンツ復号部の構成要素である暗号化ライセンス復号部１０１について詳しく説明する。構成を図１７に、その処理の流れを図１９に示す。

【００６９】以下、図１９に示すフローチャートを参照して、暗号化ライセンス復号部１０１について説明する。

【００７０】暗号化デジタルライセンス情報Ｌが入力すると（ステップＳ９１）、まずデジタル署名検出部１０１ａにおいてデジタル署名の検出が行なわれる（ステップＳ９２）。すなわち、デジタル署名の検出はライセンスヘッダ中のデータを用い、例えば、次式を用いてデジタル署名の先頭アドレスを算出する。

【００７１】デジタル署名の先頭アドレス＝暗号化デジタルライセンス情報の先頭アドレス＋（ライセンスヘッダ長＋コンテンツ鍵の長さ＋コンテンツ利用条件の長さ＋認証子の長さ）

デジタル署名検証鍵取得部１０１ｂは、このデジタル署名の先頭アドレスから固定長のデジタル署名ヘッダを取得し（図６、図７参照）、そこに記載されているデジタル署名の全体長、署名の種類、署名検証鍵の番号から署名アルゴリズム及びその検証鍵を特定することができる。署名の種類、署名検証鍵の番号が取得できたら、それをもとに、デジタル署名検証鍵保持部１０１ｆを検索し、当該署名の種類、署名検証鍵の番号に対応する署名アルゴリズム、検証鍵を取得する（ステップＳ９４）。

【００７２】デジタル署名（ヘッダ）が検出できなかった場合は、エラー出力して処理を終了する（ステップＳ９３、ステップＳ１０１）。

【００７３】デジタル署名が検出できたら、次に、デジタル署名検証部１０１ｃは、検出されたデジタル署名を、デジタル署名ヘッダにて指定された署名アルゴリズムと署名検証鍵番号の署名検証鍵を使って検証する（ステップＳ９５）。

【００７４】ここでのデジタル署名は公開鍵暗号によるそれを考えている。即ち、署名作成鍵（秘密鍵）を持っている認可されたサーバもしくは販売店のみが、公的複製コンテンツに対応するライセンスファイルが作成できる。それ以外の者は例え再生装置を所有していても、その中にあるのは署名検証鍵（公開鍵）だけであり、公開鍵から秘密鍵を求めることが難しいのが公開鍵暗号の安全性であるので、充分安全な公開鍵暗号を使えば、秘密鍵を知らない第三者はライセンスに対応したデジタル署名は作成できないことになる。このことから公的複製コンテンツに対応したライセンスが作れるのは認可された

販売者であることが導かれる。しかし一方で、公開鍵暗号も攻撃法（解読法）の発展によりいつまでも安全であるとは限らない。この点に鑑みて、デジタル署名のヘッダの中で署名アルゴリズム、署名検証鍵を指定して随時サーバ側で変更できるような構成となっている。

【００７５】デジタル署名検証部１０１ｃで署名検証結果がＮＧと判断された場合はエラー出力する（ステップＳ９６、ステップＳ１０２）。そうでない場合は、ライセンス鍵生成部１０１ｄは、暗号化コンテンツが記録されているメディアのメディアＩＤ（ＭＩＤ）を取得し（ステップＳ９７）、これを再生装置の中に秘密に保持された関数を用いて、

ｗ＝ｆ（ＭＩＤ）

からメディアに依存したライセンス鍵ｗを得る（ステップＳ９８）。

【００７６】これはコンテンツを別メディアに移す、即ちコピーした場合、メディアに依存したライセンス鍵ｗしか得られないため、暗号化デジタルライセンス情報が復号できなくなり、この結果としてコンテンツの復号ができないようにするための仕組みである。

【００７７】このように私的複製あっても公的複製であっても、コピーのためには暗号化デジタルライセンス情報を作り直さなければならなく、それができるのは関数ｆを知る正当な記録装置だけであるためコピーの回数の制限などが確実に行なえることから不正利用を防止することができる。この意味から、関数ｆを実現するハードウエアもしくはファームウエアは耐タンパなＬＳＩの中に存在することが望ましい。

【００７８】ライセンス復号部１０１ｅは、このようにして作成されたライセンス鍵ｗを用いて暗号化デジタルライセンス情報を復号し（ステップＳ９９）、デジタルライセンス情報Ｌｏを得、それを出力する（ステップＳ１００）。

【００７９】以上が、公的複製コンテンツ再生部５の暗号化コンテンツ復号部５ｃおよびその構成要素である暗号化ライセンス復号部１０１の説明である。尚、私的複製コンテンツ再生部４の暗号化コンテンツ復号部４ｃの暗号化ライセンス復号部１０１は、図１７のデジタル署名検出部１０１ｃ、デジタル署名検証鍵取得部１０１ｂ、デジタル署名検証鍵保持部１０１ｆ、デジタル署名検証部１０１ｃは構成として必ずしも必要ではなく、それらの処理は不要である。

【００８０】次に、以上説明したコンテンツ再生装置についてのいくつかのバリエーションを述べる。

【００８１】まず、図８の全体構成において、コンテンツの種類によって再生部を完全に分離した形を示しているが、これは必ずしも必要ではない。実質上はライセンスファイルの種類によって別れ、更に前述したように処理も似ている部分も多い。このことから、同一の処理をする部分を一つの回路にすることにより、回路規模を小さくすることができる。また、逆に同じ機能を持った回路であっても仕様を再生部毎に変更しておくことで、安全性を向上させることができる。例えば、各再生部のデータ解凍部（４ｄ、５ｄ、６ｆ）では、コンテンツの種類毎に別々のアルゴリズムを使うことで、ライセンス情報によってコンテンツの種類を偽ることがより難しくなる。

【００８２】また、オリジナルコンテンツ再生部を持たない再生装置の構成も考えられる。この場合、再生装置の側でオリジナルコンテンツの再生はできなくなり、コンテンツは公的複製コンテンツと私的複製コンテンツの２つに限られることになる。このようにすることによって、自作のコンテンツでも私的複製コンテンツとして見なされるという問題点があるが。その反面、ラジオやテレビからのコンテンツのダビングなど自作コンテンツでないものをオリジナルコンテンツとして記録し無条件に再生されてしまうという問題は避けられる。

【００８３】更にデジタル署名に関しては、図１の形態で付加する以外にも、図２０に示すように、ライセンス鍵ｗでの暗号化の上からさらに署名生成鍵Ｋｓで再暗号化を行っても良い。このようにしても、異なった署名生成鍵で暗号化しても、正しい署名検証鍵で復号しても正しく復号できないように構成することができる。正しく復号できたかどうかの判定は認証子ＭＡＣによって確実に判定できる。このようにすることによってデジタル署名分のデータサイズが削減できる。

【００８４】（第２の実施形態）ここでは、自作のコンテンツからオリジナルコンテンツもしくは私的複製コンテンツ、公的複製コンテンツからは私的複製コンテンツを製作することができるコンテンツ記録装置について説明する。

【００８５】本実施形態は、前述した第１の実施形態の再生装置に対応した記録装置であり、当該再生装置と一体化し、コンテンツ記録再生装置を構成することができる。

【００８６】本実施形態に係るコンテンツ記録装置の全体構成を図２１に、その処理の流れを図２４のフローチャートに示している。以下、図２４のフローチャートを参照しながら図２１のコンテンツ再生装置について説明する。

【００８７】コンテンツ入力部２０２には、コンテンツとして暗号化されたコンテンツ（Ｋｃ［Ｃ］）もしくは暗号化されていないコンテンツＣが暗号化ライセンス情報Ｌとともに入力される（ステップＳ２０１）。

【００８８】全体制御部２０１は、暗号化デジタルライセンス情報のライセンスヘッダを参照して、当該コンテンツが公的複製コンテンツであれば（ステップＳ２０２）、私的複製コンテンツ作成部２０４にこれらのデータを送り、私的複製コンテンツ作成処理に進む（ステップＳ２０３）。

【００８９】当該コンテンツが私的複製コンテンツであれば（ステップＳ２０４）、私的複製コンテンツ作成部２０４にこれらのデータを送り、私的複製コンテンツ作成処理に進む（ステップＳ２０５）。

【００９０】当該コンテンツがオリジナルコンテンツであれば（ステップＳ２０６）、オリジナルコンテンツ作成部２０５にこれらのデータを送り、オリジナルコンテンツ作成処理を開始する（ステップＳ２０７）。

【００９１】このようにコンテンツの種類により記録手段を変更し、記録装置では高々私的複製しかできないような環境を提供することにより、正式な販路に載った公的複製コンテンツと私的複製コンテンツを差別化し、公的複製コンテンツの価値を相対的に上げることにより、公的複製コンテンツの販路の拡大に寄与する。

【００９２】次に、図２１のコンテンツ記録装置の私的複製コンテンツ作成部２０４に関して詳しく説明する。図２２に私的複製コンテンツ作成部２０４の構成例を、その処理の流れを図２５～図２６に示す。

【００９３】以下、図２５～図２６に示すフローチャートを参照して、私的複製コンテンツ作成部２０４について説明する。

【００９４】私的複製コンテンツを複製する際、まず、コンテンツ入力部２０４ｂから暗号化コンテンツＫｃ［Ｃ］と、その暗号化デジタルライセンス情報Ｌと、複製形態情報Ｑが入力され、処理が開始される（ステップＳ２１１）。

【００９５】複製形態情報Ｑとは図３０に示す構造をしている。すなわち、複製形態情報Ｑは複製後のコンテンツ種別（複製コンテンツ種別）と、複製コンテンツの利用条件（利用条件情報）とが記載されている。

【００９６】ここで、利用条件情報は、図３１に示す構成をしており、デジタル出力フラグ、有効期限情報、有効利用回数情報、コピー回数制限情報からなり、それぞれデジタルライセンス情報、アナログライセンス情報に記載されている情報に埋め込むための情報である。

【００９７】なお、以下の処理でも明らかになるように、複製後のコンテンツ種別により、必ずしもこれらの情報がそのまま反映される訳ではない。後にも説明するようにこれは複製後のコンテンツ種別により、各上限値が規定されており、この上限値を越えて設定することを許さないためである。このことにより私的複製コンテンツ、公的複製コンテンツ、オリジナルコンテンツに利用上の区別を付け、コンテンツ供給業者の利益にかなったシステムを実現する。

【００９８】さて、入力された暗号化コンテンツＫｃ［Ｃ］と、その暗号化デジタルライセンス情報Ｌと、複製形態情報Ｑとは、制御部２０４ａに送られ、暗号化コンテンツＫｃ［Ｌ］と暗号化デジタルライセンス情報Ｌはコンテンツ復号部２０４ｅに送られる。

【００９９】コンテンツ復号部２０４ｅでは、第１の実施形態のコンテンツ再生装置のコンテンツ再生と同様にして、暗号化コンテンツを復号する。すなわち、ソース側のメディアＭからメディアＩＤ取得部２０６を経由してメディアＩＤ（ＭＩＤ）を取得し（ステップＳ２１２）、当該メディアＩＤと秘匿された関数ｆとを用いて、

ｗ＝ｆ（ＭＩＤ）

という関係式からライセンス鍵ｗを作り（ステップＳ２１３）、暗号化デジタルライセンス情報Ｌを復号する（ステップＳ２１４）。復号されたデジタルライセンス情報からコンテンツ復号鍵Ｋｃを抽出する（ステップＳ２１５）。さらに、デジタルライセンス情報から認証子を抽出し、これを検査することによってコンテンツ復号鍵Ｋｃに誤りがないことを確認する（ステップＳ２１６）。そして、コンテンツ復号鍵Ｋｃを用いて暗号化コンテンツを復号し、コンテンツＣを得る（ステップＳ２１８）。

【０１００】コンテンツ復号部２０４ｅで復号されたコンテンツＣは、制御部２０４ａを経由してアナログライセンス検出・修正部２０４ｆに送られる。ここでは、まず、データ解凍部２０４ｇにコンテンツＣを送り、コンテンツＣの圧縮を解凍し（ステップＳ２１９）、解凍されたデジタルコンテンツＣに対して、Ｄ／Ａ変換を行ない（ステップＳ２２０）、アナログコンテンツＣａを得る。このアナログコンテンツＣａからアナログライセンス情報を抽出し（ステップＳ２２１）、アナログライセンス情報の複製情報により、当該コンテンツの種類を特定する。

【０１０１】当該ソースのコンテンツが公的複製コンテンツであった場合（ステップＳ２２２）、図５に示すようなアナログライセンス情報の複製情報を私的複製コンテンツと修正し（ステップＳ２２６）、同じくアナログライセンス情報のコピー回数制限情報を私的複製コンテンツに許された上限値に設定する（ステップＳ２２７）。

【０１０２】一方、当該ソースのコンテンツが私的複製コンテンツの場合は（ステップＳ２２３）、図５に示すようなアナログライセンス情報のコピー回数制限情報を「１」減算する（ステップＳ２２４）。

【０１０３】また、当該ソースのコンテンツが公的複製コンテンツでも私的複製コンテンツでもない場合、エラー出力をする（ステップＳ２２８）。

【０１０４】以上の処理で作成されたアナログライセンス情報を現在記録されているアナログライセンス情報を消去して、アナログコンテンツに埋め込む（ステップＳ２２５）。さらに、Ａ／Ｄ変換してデジタルコンテンツＣｄに変換した後（ステップＳ２２９）、データ圧縮部２０４ｈに送り圧縮処理を行なって（ステップＳ２３０）、新しいコンテンツＣを得る。

【０１０５】新しいコンテンツＣは、アナログライセン

ス情報検出・修正部２０４ｆから制御部２０４ａを経由して、コンテンツ暗号化部２０４ｄへコンテンツ暗号鍵Ｋｃとともに送られる。

【０１０６】コンテンツ暗号化部２０４ｄでは、入力されたコンテンツＣを同じく入力されたコンテンツ復号鍵Ｋｃで暗号化し、暗号化コンテンツＫｃ［Ｃ］を得る（ステップＳ２３１）。

【０１０７】一方、制御部２０４ａでは、複製形態情報Ｑの利用条件情報に記載されているデジタル出力フラグ、有効期限情報、有効利用回数制限を参照し、これらの条件が私的複製コンテンツの範囲を逸脱していないことを確認する。逸脱していた場合は私的複製コンテンツにおいて認められている範囲でデジタルライセンス情報に含まれるコンテンツ利用条件Ｕを作成する（ステップＳ２３２）。

【０１０８】次に、コンテンツ復号鍵Ｋｃとコンテンツ利用条件Ｕとから認証子（ＭＡＣ）を計算する（ステップＳ２３３）。計算の方式は前述した第１の実施形態のコンテンツ再生装置で認証子確認のために行なった計算と同じである。

【０１０９】さらに、ライセンスヘッダの複製情報の部分に私的複製コンテンツである旨の情報その他を算出して格納し、当該コンテンツのデジタルライセンス情報が完成する。

【０１１０】次に、デジタルライセンス情報の暗号化のためターゲット側（記録側）メディアＭ’からメディアＩＤ取得部２０６を通じてメディアＩＤ（ＭＩＤ）を取得する（ステップＳ２３５）。取得されたメディアＩＤ（ＭＩＤ）から

ｗ＝ｆ（ＭＩＤ）

によってライセンス鍵ｗを生成する（ステップＳ２３６）。この生成方式は前述したコンテンツ復号部２０４ｅの処理の部分で述べた暗号化デジタルライセンス情報Ｌの際に作成したライセンス鍵の作成方式と同じである。だが前者の場合とはＭＩＤが異なるので異なるライセンス鍵が生成される。

【０１１１】このように複製の前後で暗号化デジタルライセンス情報のデータを変更することで、不正な複製を防ぐことができるのである。

【０１１２】ステップＳ２３６で得られたライセンス鍵ｗを使ってデジタルライセンス情報Ｌｏを暗号化して暗号化デジタルライセンス情報Ｌを得る（ステップＳ２３７）。

【０１１３】以上によって記録すべきデータは全て完成し、暗号化コンテンツＫｃ［Ｃ］と暗号化デジタルライセンス情報Ｌとをそれぞれコンテンツ記録部２０８、ライセンス記録部２０７を通じてターゲット側メディアＭ’に記録する（ステップＳ２３８～ステップＳ２３９）。

【０１１４】次に、図２１のコンテンツ記録装置の中のオリジナルコンテンツ作成部２０５に関して詳しく説明する。オリジナルコンテンツ作成部２０５の構成を図２３に、その処理の流れを図２７～図２９に示す。

【０１１５】以下、図２７～図２９に示すフローチャートを参照して、図２３のオリジナルコンテンツ作成部２０５について説明する。

【０１１６】オリジナルコンテンツを複製する際、まず、コンテンツ入力部２０５ｂからコンテンツＣと複製形態情報Ｑが入力され、処理が開始される（ステップＳ２４１）。

【０１１７】コンテンツＣが制御部２０５ａを経由して、アナログライセンス情報検出修正部２０５ｄに送られ、ここからデータ解凍部２０５ｇの処理によりコンテンツの解凍が行なわれる（ステップＳ２４２）。

【０１１８】解凍されたデジタルコンテンツＣｄにＤ／Ａ変換を施し、アナログライセンス情報を検出する（ステップＳ２４３～Ｓ２４４）。ここでオリジナルコンテンツであれば検出されないはずであるが、データの一部を改竄することにより、当該コンテンツをオリジナルコンテンツになりすまして入力していた場合などはここでエラー出力し、処理を終了する（ステップＳ２４５～ステップＳ２４６）。

【０１１９】オリジナルコンテンツであった場合、次に複製先をオリジナルコンテンツとするのか私的複製コンテンツとするのかを複製形態情報Ｑの複製コンテンツ種別によって判断する（ステップＳ２４７）。

【０１２０】オリジナルコンテンツは、先に定義したように利用者自身に著作権のあるコンテンツを考えているので暗号化しないオリジナルコンテンツにも私的複製コンテンツにも複製できる。当然オリジナルコンテンツに複製した方がより有利な条件で再生できるが、著作者自身が複製先で利用形態に何らかの制限を設けたい場合は私的複製コンテンツとして記録することによって目的は実現される。

【０１２１】私的複製コンテンツとして複製したい場合は、ステップＳ２４８へ進み、アナログライセンス情報をコンテンツに記録する必要がある。このためアナログライセンス情報を作成し、その複製情報を私的複製とし、コピー回数制限を利用形態情報Ｑに含まれるコピー回数制限情報を私的複製コンテンツで許可されているコピー回数の上限値を越えない範囲で設定し、当該アナログライセンス情報をコンテンツＣに埋め込み、Ａ／Ｄ変換し、更に、データ圧縮部２０５ｈで圧縮処理を施すことにより新たなコンテンツＣを得る（ステップＳ２４８～ステップＳ２５２）。

【０１２２】一方、オリジナルコンテンツとして複製する場合には、ステップＳ２４７からステップＳ２５１へ進み、アナログライセンス情報の修正処理をすることなしにＡ／Ｄ変換を行ない、圧縮処理を行なってコンテンツＣを得る（ステップＳ２５１～ステップＳ２５２）。

【０１２３】以上の処理で作成されたコンテンツＣはアナログライセンス情報検出修正部２０５ｄから制御部２０５ａへ送られ、制御部２０５ａで複製形態情報Ｑを参照して私的複製コンテンツに複製するか、オリジナルコンテンツに複製するかによって処理手順を変える（ステップＳ２５３）。

【０１２４】まず、オリジナルコンテンツに複製する場合は、暗号化する必要がないので、ライセンス生成部２０５ｃは、デジタルライセンス情報をライセンスヘッダのみ作成し、ライセンスヘッダ中の複製情報を「オリジナルコンテンツ」とし（ステップＳ２６４）、ライセンス記録部２０７を通じて当該デジタルライセンス情報をターゲット側のメディアに記録する（ステップＳ２６２）。ここでオリジナルコンテンツの場合のデジタルライセンス情報はライセンスヘッダのみ存在するため暗号化部分はなく、ライセンス鍵も作成しなくても良い。また、コンテンツＣも暗号化する必要がないのでそのままコンテンツ記録部２０８を通し、ターゲット側のメディアに記録される（ステップＳ２６３）。

【０１２５】次に、私的複製コンテンツとして記録する場合の処理に関して述べる。私的複製コンテンツとして記録する場合は（ステップＳ２５３）、コンテンツＣを暗号化し、しかも当該コンテンツに対応したコンテンツ復号鍵Ｋｃが含まれる暗号化デジタルライセンス情報Ｌを作成し、メディアに記録しなくてはならない。順次その手順を説明する。

【０１２６】制御部２０５ａは、コンテンツＣをコンテンツ暗号化部２０５ｅに送り、コンテンツ暗号化部２０ｅでは、コンテンツ復号鍵生成部２０５ｆに命令を出し、コンテンツ鍵Ｋｃを作成させる（ステップＳ２５４）。作成されたコンテンツ復号鍵Ｋｃでコンテンツ Ｃを暗号化し（ステップＳ２５５）、暗号化コンテンツＫｃ［Ｃ］を得る。この暗号化コンテンツＫｃ［Ｃ］は、コンテンツ記録部２０８に渡され、ターゲット側のメディアに記録される（ステップＳ２６３）。

【０１２７】一方、コンテンツ復号鍵Ｋｃは、一端、制御部２０５ａに渡された後、ライセンス生成部２０５ｃに渡される。ライセンス生成部２０５ｃでは、メディアＩＤ取得部２０６からターゲット側のメディアのメディアＩＤ（ＭＩＤ）を取得し（ステップＳ２５６）、

ｗ＝ｆ（ＭＩＤ）

によりライセンス鍵ｗを作成する（ステップＳ２５７）。

【０１２８】また、デジタルライセンス情報に含まれるコンテンツ利用条件Ｕを複製形態情報Ｑの利用条件情報を参照し、私的複製コンテンツに認められた範囲で決定する（ステップＳ２５８）。

【０１２９】次に、コンテンツ鍵Ｋｃと利用条件Ｕとから認証子（ＭＡＣ）を生成する（ステップＳ２５９）。これによってデジタルライセンス情報Ｌｏを生成し（ステップＳ２６０）、先に生成したライセンス鍵ｗを使ってデジタルライセンス情報を暗号化して、暗号化デジタルライセンス情報Ｌを得る（ステップＳ２６１）。

【０１３０】得られた暗号化デジタルライセンス情報Ｌをライセンス記録部２０７によってターゲット側のメディアに記録する（ステップＳ２６２）。

【０１３１】以上で、コンテンツ記録装置の説明を終える。

【０１３２】次に、上記第２の実施形態のいくつかの変形例（第３～第６の実施形態）について述べる。

【０１３３】（第３の実施形態）オリジナルコンテンツ以外（とくに公的複製コンテンツ）を複製する際には、私的複製コンテンツ作成部２０４では、当該コンテンツを適度に劣化させることが望ましい。これは劣化によって複製への期待が薄れ、正式な販路にのった公的複製コンテンツの販売が促進されるからである。この意味でアナログライセンス情報検出修正部２０４ｆにおいてコンテンツにノイズを載せるかデータ圧縮における圧縮率を上げるかによってこれを実現する構成も考えられる。このためにはデータ圧縮部２０４ｈの圧縮率を調整して劣化が起こる程度にする方法もしくはアナログライセンス情報を埋め込む際に埋め込みを極端にしてコンテンツの劣化がおこる程度までにする方法が考えられる。特に後者の場合、アナログライセンス情報が剥離させにくくなるというメリットもある。

【０１３４】（第４の実施形態）コンテンツの種類としてオリジナルコンテンツを認めない記録装置（もしくは記録再生装置）も考えられる。このような装置は、例えば、図２１の構成において、オリジナルコンテンツ作成部２０５を省き、上記説明のうち、オリジナルコンテンツの入力およびオリジナルコンテンツでの複製に関する処理を省けばよい。

【０１３５】逆に、少なくともオリジナルコンテンツの入力を認める場合、オリジナルコンテンツとして認める入力端子を限定する方法が考えられる。この方法によれば、例えば、マイク端子から入力される音声はオリジナルコンテンツとして記録できるが、ラジオ端子から入力される音声は私的複製コンテンツとして記録させるような機構を取ると、入力媒体によって複製コンテンツの種類を決定することができ、例え本記録装置のフォーマットで入力されていなくても記録することができるばかりか、当該複製がオリジナルコンテンツからのものなのかそうでないのかを区別することができる。

【０１３６】（第５の実施形態）第１の実施形態のコンテンツ再生装置と第２の実施形態のコンテンツ記録装置はそれぞれ独立の機構を有しているが、一体化した形態の記録再生装置を考えることも可能である。この場合、同じ機能を持つ構成要素であるメディアＩＤ取得部、データ圧縮部、データ解凍部などを共通化することも可能である。

【０１３７】（第６の実施形態）記録されるソースコンテンツをアナログのみに限り、私的複製コンテンツへの複製しか許さないという形態も存在する。このようにすることによって、デジタルコンテンツを記録する際、一端アナログレイヤを経由することによって、コンテンツの質的劣化を引き起こすことができ、従来の私的複製と同程度の質の劣化が実現され、コンテンツの質の上での私的複製が実現できる。

【０１３８】このようなコンテンツ記録装置の構成を図３２に、その処理の流れを図３３～図３４に示す。

【０１３９】以下、図３２のコンテンツ記録装置について、図３３～図３４に示すフローチャートを参照して説明する。

【０１４０】コンテンツ入力部３０１からアナログコンテンツＣａが入力される（ステップＳ３０１）。入力されたアナログコンテンツＣａは、アナログライセンス情報検出修正部３０２に送られ、そこでアナログライセンス情報が抽出され（ステップＳ３０２）、アナログライセンス情報に含まれるコピー回数制限が「１」以上であることを確認する（ステップＳ３０３）。そうでなかった場合はこれ以上複製は生成できないのでエラー出力する（ステップＳ３０４）。

【０１４１】以下、アナログライセンス情報が存在しないか、コピー回数制限が「１」以上であるとする。アナログライセンス情報がない場合、コピー回数制限は私的複製コンテンツの上限値に設定し、あった場合はコピー回数制限を「１」減じ、いずれの場合も複製情報を私的複製コンテンツに設定したアナログライセンス情報を作成し、アナログライセンス情報が既に存在する場合はそれを取り除いた後、新たに作成されたアナログライセンス情報をコンテンツに埋め込む（ステップＳ３０５～ステップＳ３０６）。

【０１４２】アナログライセンス情報が埋め込まれたコンテンツＣａはＡ／Ｄ変換部３０３に送られ、デジタルコンテンツＣｄに変換する（ステップＳ３０７）。デジタルコンテンツＣｄは、データ圧縮部３０５に送られ、圧縮されたコンテンツＣを作成する（ステップＳ３０８）。

【０１４３】コンテンツＣは、全体制御部３０４を経由してコンテンツ暗号化部３０７へ送られ、コンテンツ暗号化部３０７では、コンテンツ鍵生成部３０９で生成されたコンテンツ復号鍵Ｋｃを使って、コンテンツＣを暗号化し、暗号化コンテンツＫｃ［Ｃ］を作成する（ステップＳ３０９～ステップＳ３１０）。

【０１４４】コンテンツ暗号化部３０７は、一方でコンテンツ復号鍵Ｋｃを全体制御部３０４に送り、全体制御部３０４が決める利用条件Ｕとともにライセンス生成部３０６に送る。

【０１４５】ライセンス生成部３０６では、コンテンツ復号鍵Ｋｃと利用条件Ｕから認証子（ＭＡＣ）を生成し、デジタルライセンス情報Ｌｏを作成する。生成されたデジタルライセンス情報Ｌｏは、ライセンス暗号化部３０８に送られ、ライセンス暗号化部３０８ではライセンス鍵生成部３１０で生成されたライセンス鍵ｗを使ってデジタルライセンス情報Ｌｏを暗号化する（ステップＳ３１１～ステップＳ３１４）。

【０１４６】ここで、ライセンス鍵生成部３１０の処理の流れを説明する。ライセンス鍵生成部３１０では、メディアＩＤ取得部３１２を経由して暗号化コンテンツを記録するメディアのメディアＩＤ（ＭＩＤ）を取得し（ステップＳ３１２）、

ｗ＝ｆ（ＭＩＤ）

により、ライセンス鍵ｗを生成する（ステップＳ３１３）。

【０１４７】さて、暗号化デジタルライセンスＬは、ライセンス記録部３１１を経て、メディアに記録される（ステップＳ３１５）。同様に、暗号化コンテンツＫｃ［Ｃ］もメディアに記録される（ステップＳ３１６）。

【０１４８】第１の実施形態でも述べたオリジナルコンテンツを許さない再生装置を本実施形態の記録装置と一体化するか、もしくは対として使うことによって、よりセキュリティの高いコンテンツ記録再生装置が作成できる。即ち、本発明の記録再生装置以外からのコンテンツを入力して記録する際にはアナログ入力しか認められず、デジタルコンテンツの記録には私的複製コンテンツに制限されるからである。このことは即ち、デジタルでの記録再生の世界であっても一端アナログを経由するため、従来からの記録再生システム以上の品質向上は望めないことを意味しており、複製の抑止力となると同時に公的複製コンテンツの価値を相対的に上げ、公的複製コンテンツの販売市場を確保することがより確実にできる。

【０１４９】（第７の実施形態）本実施形態では、デジタルコンテンツを購入再生する際に利用するコンテンツ販売装置とコンテンツ購入装置について説明する。ここでは、例えば、デジタルコンテンツをインターネットサーバ或は自動販売機経由で購入／販売する仕組みの一形態を示す。

【０１５０】まず、コンテンツ販売装置の実施形態を説明する。コンテンツ販売装置とは購入要求に応じて公的複製コンテンツを作成し、販売する販売装置を言う。本実施形態では、ネットワーク上に実現された電子商店が開設するコンテンツ販売サーバ装置を想定している。

【０１５１】図３５は販売サーバの全体構成図、図３６は、図３５中のライセンス生成部４０３の構成図である。

【０１５２】まず、販売サーバの全体の処理の流れを示す図３７と図３８を参照して説明する。

【０１５３】販売サーバはクライアントからのコンテンツ購入要求を受信することによって動作を開始する（ス

テップＳ４０１）。購入要求情報は図３９に示すように、購入申込をした顧客のＩＤ情報と、購入したいコンテンツのコンテンツＩＤ（ＣＩＤ）、購入利用条件、（Ｕｃ）、顧客がコンテンツを記録する記録メディアのメディアＩＤ（ＭＩＤ）、クライアントアドレスからなっている。

【０１５４】販売サーバは、購入要求情報を受信すると、これを全体制御部４０２へ送り、購入要求情報に含まれているコンテンツＩＤをコンテンツ検索部４０５に送り、コンテンツデータベース（ＤＢ）４０７を検索して、コンテンツ復号鍵Ｋｃと販売金額Ｐ（と場合によっては、暗号化コンテンツＫｃ［Ｃ］）を抽出する（ステップＳ４０２）。

【０１５５】ここで、暗号化コンテンツＫｃ［Ｃ］を取り出す条件として、例えばコンテンツＩＤが十分大きなビット数で表現されており、冗長なビットが存在するならば冗長ビットのうちの１ビットを暗号化コンテンツを送信するか否かの判別フラグとすることができる。

【０１５６】次に（もしくはコンテンツ検索部４０５における処理と同時に）、全体制御部４０２は、顧客ＩＤをキーに顧客のクレジット番号を顧客データベース（ＤＢ）４０８から検索し、検索されたクレジット番号で信用照会を行なう（ステップＳ４０３ステップＳ４０４）。信用照会の結果支払が可能ならば、以下で詳しく述べる手順に従って暗号化デジタルライセンス情報を生成し、暗号化デジタルライセンス情報をクライアントのアドレスに出力する（ステップＳ４０５～ステップＳ４０７）。信用照会の結果支払が不可能である場合は、その旨クライアントのアドレスへ通知する。通知及び出力は電子メールによっても良いし、直接ネットワーク接続されている場合には、接続されているネットワークを使えば良い。

【０１５７】次に、図３６のライセンス生成部４０３の暗号化デジタルライセンス情報の生成処理について、図３８に示すフローチャートを参照して説明する。

【０１５８】ライセンス生成部４０３は、コンテンツＤＢ４０７から出力されたコンテンツ復号鍵Ｋｃと購入要求情報から抽出されたメディアＩＤ（ＭＩＤ）との入力を受けて処理を開始する（ステップＳ４１１）。

【０１５９】まず、ライセンス生成部４０３内の制御部４０３ｂによって入力された利用条件Ｕを決定し、コンテンツ復号鍵Ｋｃと利用条件Ｕから認証子（ＭＡＣ）を生成して、デジタルライセンス情報Ｌｏを作成する（ステップＳ４１２～ステップＳ４１３）。

【０１６０】次に、入力されたメディアＩＤ（ＭＩＤ）より

ｗ＝ｆ（ＭＩＤ）

によってライセンス鍵ｗを生成する（ステップＳ４１４）。ライセンス鍵生成部４０３ｃは、ライセンス鍵ｗとデジタルライセンス情報Ｌｏを制御部４０３ｂに送り、制御部４０３ｂでは、ライセンス情報Ｌｏを暗号化することによって暗号化デジタルライセンス情報を生成する（ステップＳ４１５～ステップＳ４１６）。

【０１６１】さらに、サーバ秘密鍵データベース（ＤＢ）４０９から鍵サーバ秘密鍵Ｋｓと、その秘密鍵のＩＤ（ＫＩＤ）を抽出し（ステップＳ４１７）、暗号化ライセンス情報Ｌに秘密鍵Ｋｓでデジタル署名を施し（ステップＳ４１８）、これを付加して暗号化ライセンＬを作成する。そして作成されたデジタルライセンス情報Ｌを出力して処理を終える（ステップＳ４１９）。

【０１６２】ここで、デジタル署名の作成は公開鍵暗号で行ない、図６と図７に示すデータを作成する。デジタル署名ヘッダに含まれるデジタル署名全体長には当該ヘッダを含むデジタル署名の長さを、署名の種類には署名方式の種類の識別子を、署名検証鍵番号には秘密鍵のＩＤ（ＫＩＤ）をそれぞれ入力する。

【０１６３】以上で、コンテンツ販売装置、すなわち、販売サーバの説明を終了し、次に、販売に対応したコンテンツ購入装置の仕組みを説明する。コンテンツ購入装置は再生装置そのもののこともあるが、必ずしもその必要はなく、ネットワーク接続できるパーソナルコンピュータなどの機器や専用の装置であっても良い。

【０１６４】図４０にコンテンツ購入装置の構成を示し、以下、図４１～図４２に示すフローチャートを参照して、コンテンツ購入装置について説明する。

【０１６５】コンテンツ購入装置には、コンテンツ選択インタフェース（ＩＦ）５０１を通じて、購入するコンテンツのコンテンツＩＤが入力され、全体制御部５０２に送られる（ステップＳ５０１）。コンテンツ選択ＩＦ５０１は、コンテンツＩＤをキーボードから入力する形式でも良いし、専用の検索ソフトか入力ソフトにより、ユーザが歌手名や作曲者などをキーに検索し、指定することによって入力しても良い。

【０１６６】全体制御部５０２では、コンテンツＩＤの入力を受けて、メディアＩＤ抽出部５０４を経由して当該コンテンツを記録する（もしくは既に記録されている）メディアからメディアＩＤ（ＭＩＤ）を抽出する（ステップＳ５０２）。

【０１６７】次に（もしくは同時に）、顧客情報保持部５０５から（購入者の）顧客ＩＤ、顧客アドレスを抽出し（ステップＳ５０３）、これら抽出された情報を基に図３９に示すような購入要求情報を販売サーバに送信する（ステップＳ５０４～ステップＳ５０５）。

【０１６８】なお、本実施形態では、顧客情報は顧客情報保持部５０５に格納されているが、この部分を外部からの入力に変えても同様の処理ができる。

【０１６９】また、購入要求情報に従ってコンテンツ販売装置から暗号化ライセンスＬ（コンテンツ購入装置側に暗号化コンテンツがない場合は暗号化コンテンツＫｃ［Ｃ］と共に）に送信されてきた時、コンテンツ販売装

置はこれらをメディアＩＤを抽出したメディアに記録する（ステップＳ５１１～ステップＳ５１２）。

【０１７０】以上で、コンテンツ購入装置の構成と処理の流れの説明を終了する。以上の構成からコンテンツ購入装置はコンテンツ再生装置と一体化ができることが分かる。即ち、図８に示した再生装置の構成は図４０に示した販売クライアントの構成と機能的に独立であり、両方の機能を備えた装置が構成できる。同様に第２の実施形態で述べたコンテン記録再生装置との間にも同じ関係が成り立つ。

【０１７１】このため、コンテンツ販売装置とコンテンツ購入装置を一体化させたシステムも考えられる。これは、コンテンツ情報の自動販売機のような装置であり、図３５のコンテンツ販売装置の構成にける課金部４０４を自動販売機における硬貨／紙幣検出格納装置とし、作成された暗号化ライセンスＬ（及び暗号化コンテンツ）を図４０のコンテンツ購入装置の構成におけるメディア記録部５０３を経由してメディアに記録するようにすれば実現できる。

【０１７２】このような自動販売機を実現することにより、顧客はメディアを自動販売機に持参してコンテンツ及びライセンスを購入することができる。勿論、コンテンツ購入装置単独でも自動販売機を構成できる。その場合は電話回線等によってコンテンツ販売装置に接続されなければならない。

【０１７３】

【発明の効果】以上説明したように、本発明によれば、正当な経路で複製されたコンテンツ（公的複製コンテンツ）が、正当な権限なく複製されたコンテンツよりも有利な形態で流通可能となる。その結果、公的複製コンテンツの需要を増やし、コンテンツ供給者、コンテンツ利用者、電子機器供給者に利害にかなった情報流通機構を提供できる。

【図面の簡単な説明】

【図１】デジタルライセンス情報のデータ構成の一例を示した図。

【図２】暗号化デジタルライセンス情報のデータ構成の一例を示した図。

【図３】ライセンスヘッダのデータ構成の一例を示した図。

【図４】コンテンツ利用条件のデータ構成の一例を示した図。

【図５】アナログライセンス情報のデータ構成の一例を示した図。

【図６】デジタル署名のデータ構成の一例を示した図。

【図７】デジタル署名ヘッダのデータ構成の一例を示した図。

【図８】コンテンツ再生装置の構成例を示した図。

【図９】オリジナルコンテンツ再生部の構成例を示した図。

【図１０】私的複製コンテンツ再生部の構成例を示した図。

【図１１】公的複製コンテンツ再生部の構成例を示した図。

【図１２】図８のコンテンツ再生装置の処理動作を説明するためのフローチャート。

【図１３】オリジナルコンテンツ再生処理動作を説明するためのフローチャート。

【図１４】私的複製コンテンツ再生処理動作を説明するためのフローチャート。

【図１５】公的複製コンテンツ再生処理動作を説明するためのフローチャート。

【図１６】暗号化コンテンツ復号部の構成例を示した図。

【図１７】暗号化ライセンス復号部の構成例を示した図。

【図１８】暗号化コンテンツ復号処理動作を説明するためのフローチャート。

【図１９】暗号化ライセンス復号処理動作を説明するためのフローチャート。

【図２０】暗号化デジタルライセンス情報の他の例を示した図で、デジタル署名を用いない場合を示したものである。

【図２１】コンテンツ記録装置の構成例を示した図。

【図２２】私的複製コンテンツ作成部の構成例を示した図。

【図２３】オリジナルコンテンツ作成部の構成例を示した図。

【図２４】図２１のコンテンツ記録装置の処理動作を説明するためのフローチャート。

【図２５】私的複製コンテンツ作成処理動作を説明するためのフローチャート。

【図２６】私的複製コンテンツ作成処理動作を説明するためのフローチャート。

【図２７】オリジナルコンテンツ作成処理動作を説明するためのフローチャート。

【図２８】オリジナルコンテンツ作成処理動作を説明するためのフローチャート。

【図２９】オリジナルコンテンツ作成処理動作を説明するためのフローチャート。

【図３０】複製形態情報のデータ構成の一例を示した図。

【図３１】複製形態情報中の利用条件情報のデータ構成の一例を示した図。

【図３２】コンテンツ記録装置の他の構成例を示したもので、記録するコンテンツがアナログ信号の場合を示したものである。

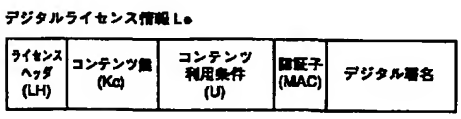
【図３３】図３２のコンテンツ記録装置の処理動作を説明するためのフローチャート。

【図３４】図３２のコンテンツ記録装置の処理動作を説

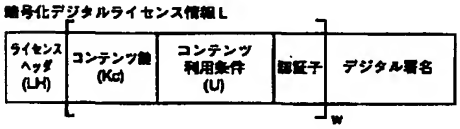
明するためのフローチャート。
【図３５】コンテンツ販売装置（販売サーバ）の構成例を示した図。
【図３６】図３５のコンテンツ販売装置のライセンス生成部の構成例を示した図。
【図３７】図３５のコンテンツ販売装置の処理動作を説明するためのフローチャート。
【図３８】ライセンス生成処理動作を説明するためのフローチャート。
【図３９】購入要求情報のデータ構成の一例を示した図。
【図４０】コンテンツ購入装置の構成例を示した図。
【図４１】図４０のコンテンツ購入装置の処理動作を説明するためのフローチャート。
【図４２】図４０のコンテンツ購入装置の処理動作を説明するためのフローチャート。
【符号の説明】
（コンテンツ再生装置）
１…全体制御部
２…コンテンツ入力部
３…再生インタフェース（ＩＦ）部
４…私的複製コンテンツ再生部
５…公的複製コンテンツ再生部
６…オリジナルコンテンツ再生部
７…デジタル出力部
８…アナログ出力部

（コンテンツ記録装置）
２０１…全体制御部
２０２…コンテンツ入力部
２０３…記録インタフェース（ＩＦ）部
２０４…私的複製コンテンツ作成部
２０５…オリジナルコンテンツ作成部
２０６…メディアＩＤ取得部
２０７…ライセンス記録部
２０８…コンテンツ記録部
（コンテンツ販売装置）
４０１…コンテンツ購入受付部
４０２…全体制御部
４０３…ライセンス生成部
４０４…課金部
４０５…コンテンツ検索部
４０６…出力部
４０７…コンテンツデータベース（ＤＢ）
４０８…顧客データベース（ＤＢ）
４０９…サーバ秘密鍵データベース（ＤＢ）
（コンテンツ購入装置）
５０１…コンテンツ選択インタフェース（ＩＦ）
５０２…全体制御部
５０３…メディア記録部
５０４…メディアＩＤ抽出部
５０５…顧客情報保持部
５０６…コンテンツ入力部

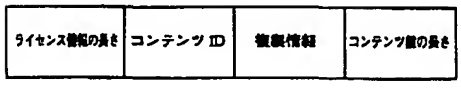
【図１】



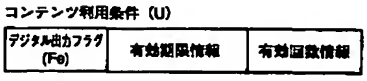
【図２】



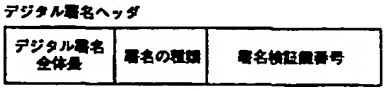
【図３】



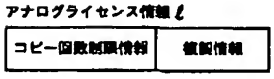
【図４】



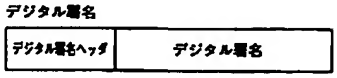
【図７】



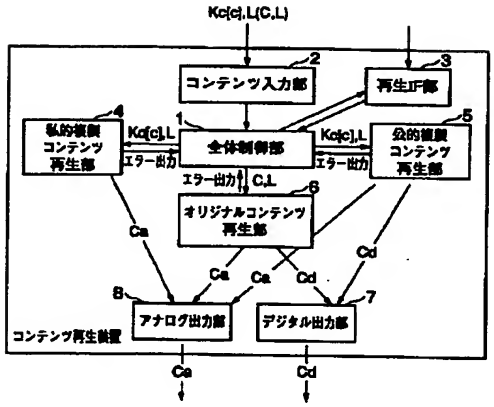
【図５】



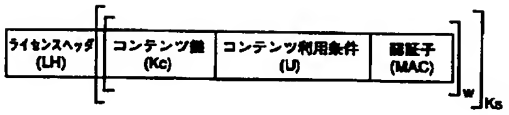
【図６】



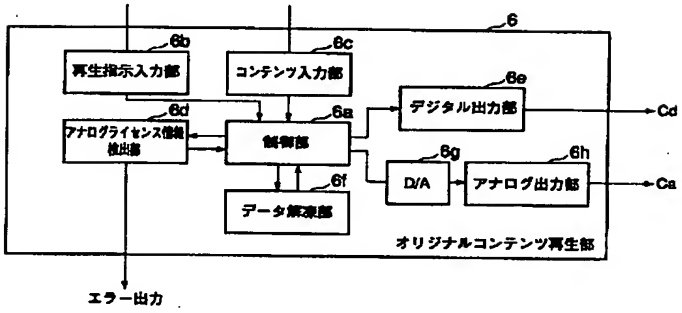
【図８】


Kc[c],L(C,L)
コンテンツ入力部
再生IF部
私的複製コンテンツ再生部
全体制御部
公的複製コンテンツ再生部
エラー出力
C,L
オリジナルコンテンツ再生部
Ca
Cd
アナログ出力部
デジタル出力部
コンテンツ再生装置

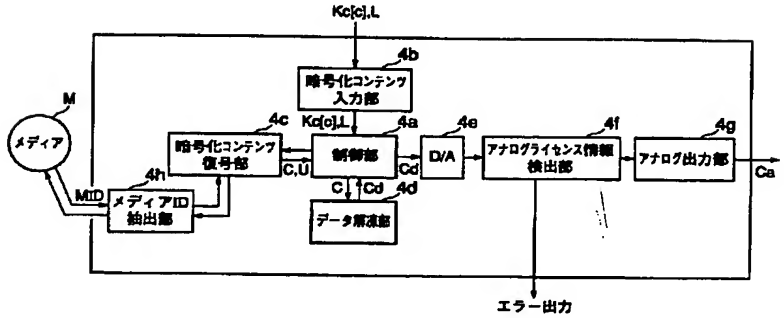
【図２０】


ライセンスヘッダ (LH)
コンテンツ鍵 (Kc)
コンテンツ利用条件 (U)
認証子 (MAC)
w
Ks

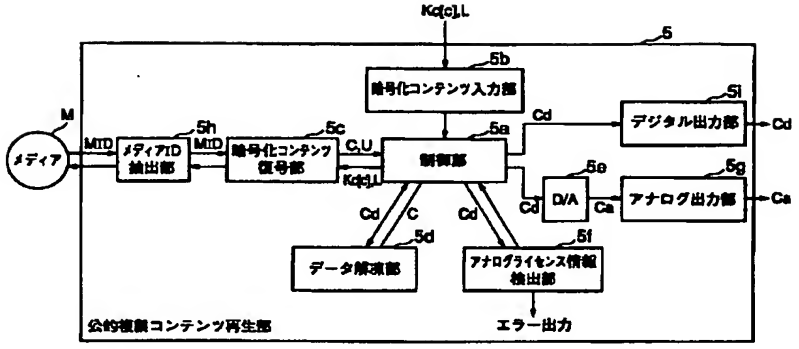
【図９】


再生指示入力部
コンテンツ入力部
アナログライセンス情報検出部
制御部
デジタル出力部
D/A
アナログ出力部
データ解凍部
オリジナルコンテンツ再生部
Cd
Ca
エラー出力

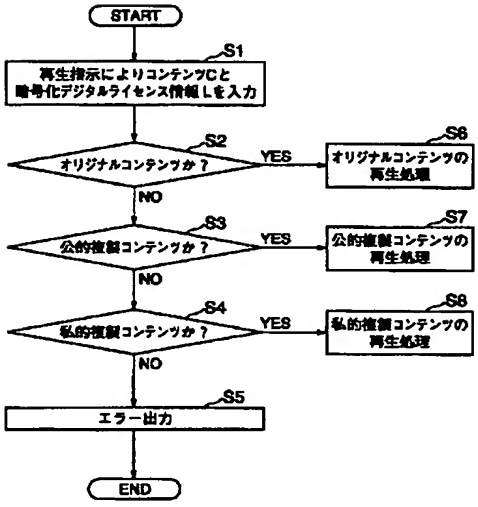
【図１０】


Kc[c],L
暗号化コンテンツ入力部
メディア
暗号化コンテンツ復号部
制御部
D/A
アナログライセンス情報検出部
アナログ出力部
MID
メディアID抽出部
データ解凍部
Ca
エラー出力

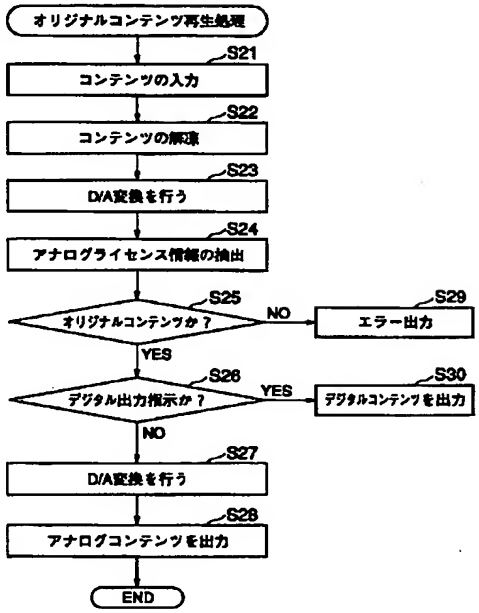
【図１１】



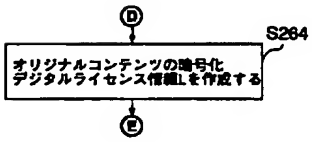
【図１２】



【図１３】



【図２９】

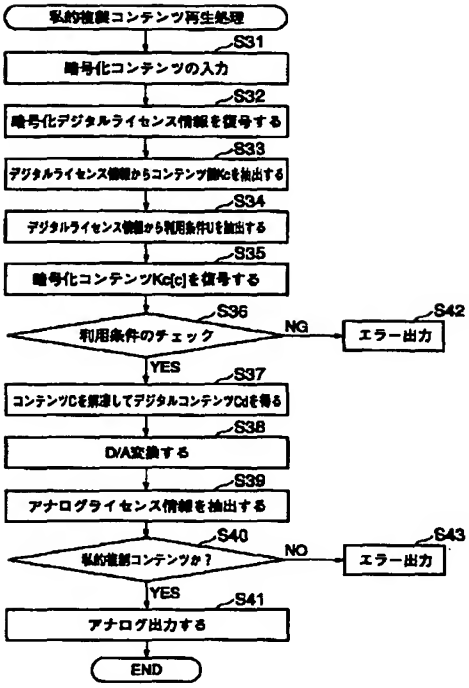


【図３０】

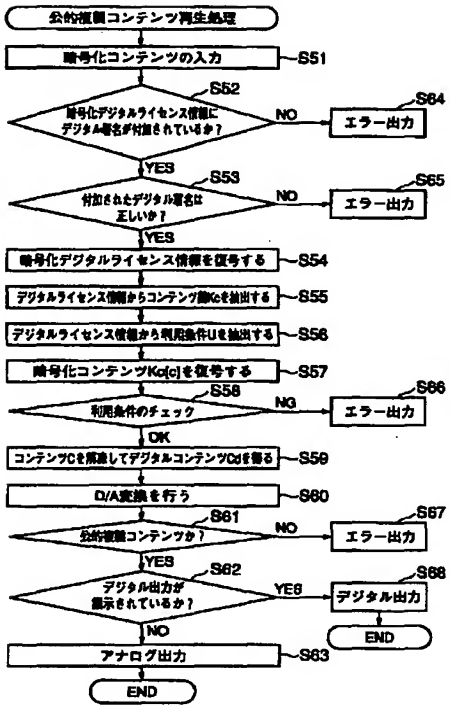
複製形態情報Q

複製コンテンツの種別	複製利用条件情報

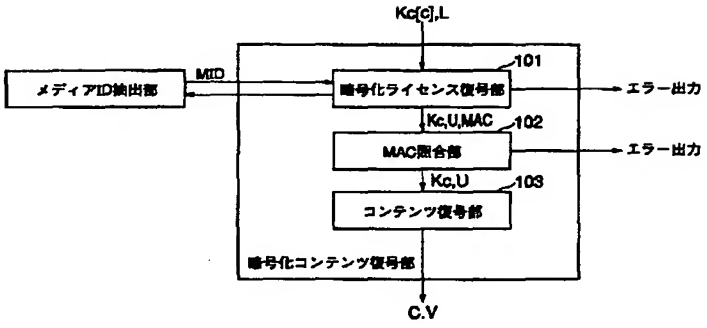
【図１４】



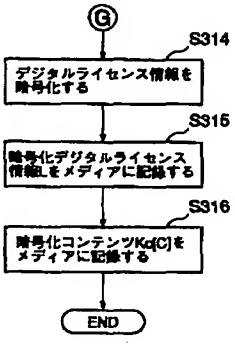
【図１５】



【図１６】



【図３４】

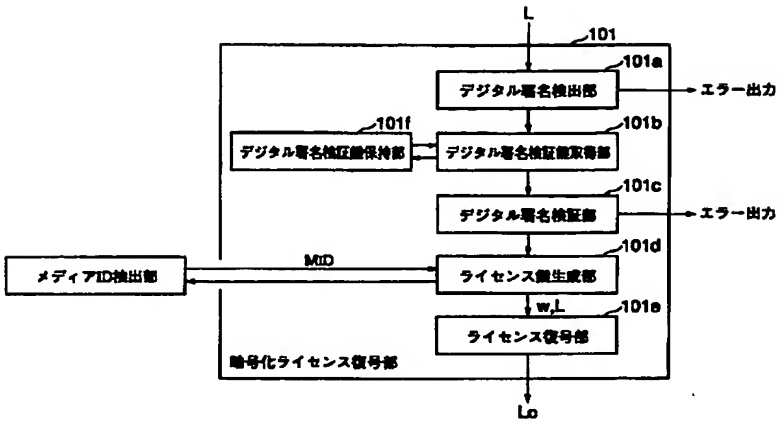


【図３１】

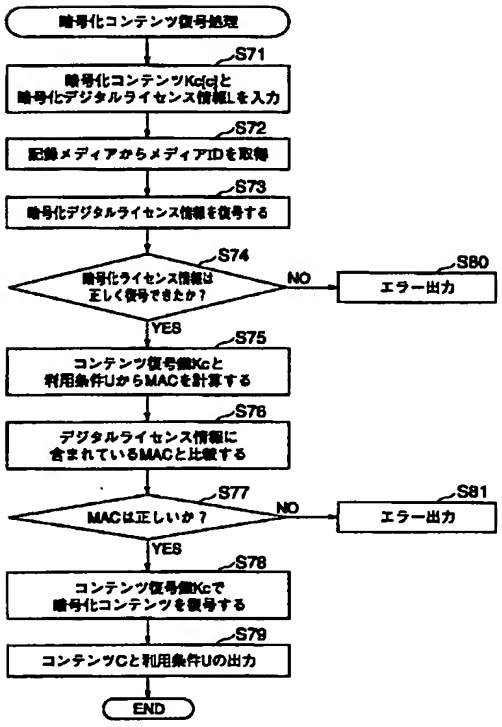
利用条件情報

デジタル出力フラグ(Fe)	有効期限情報	有効利用回数情報	コピー回数制限情報

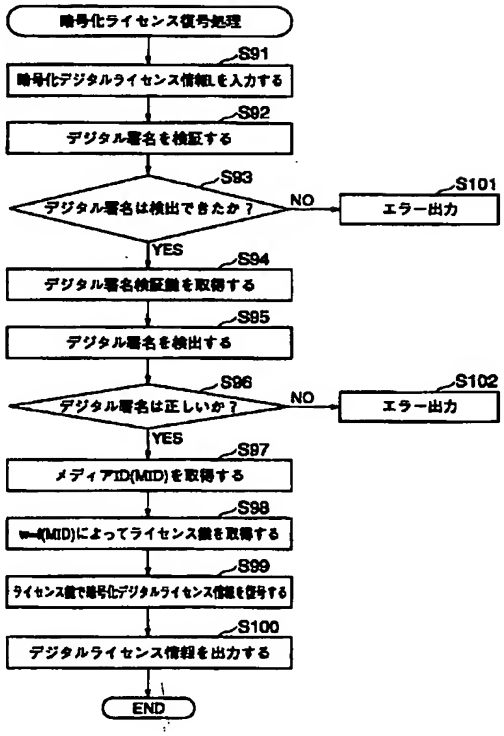
【図１７】


L
101
101a
デジタル署名検出部
エラー出力
101f
デジタル署名検証鍵保持部
101b
デジタル署名検証鍵取得部
101c
デジタル署名検証部
エラー出力
101d
メディアID検出部
MID
ライセンス鍵生成部
w,L
101e
ライセンス復号部
暗号化ライセンス復号部
Lo

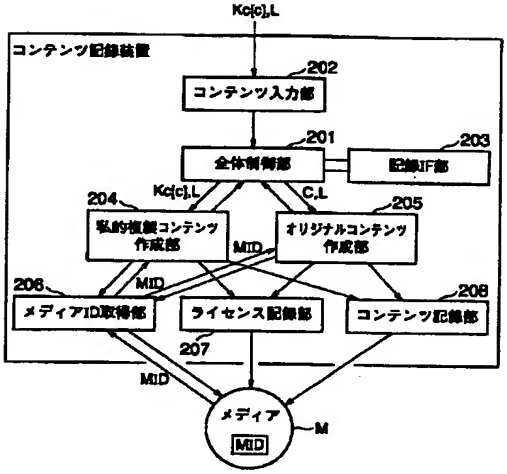
【図１８】


暗号化コンテンツ復号処理
S71
暗号化コンテンツKc[c]と
暗号化デジタルライセンス情報Lを入力
S72
記録メディアからメディアIDを取得
S73
暗号化デジタルライセンス情報を復号する
S74
暗号化ライセンス情報は
正しく復号できたか？
NO
S80
エラー出力
YES
S75
コンテンツ復号鍵Kcと
利用条件Uから MACを計算する
S76
デジタルライセンス情報に
含まれているMACと比較する
S77
MACは正しいか？
NO
S81
エラー出力
YES
S78
コンテンツ復号鍵Kcで
暗号化コンテンツを復号する
S79
コンテンツCと利用条件Uの出力
END

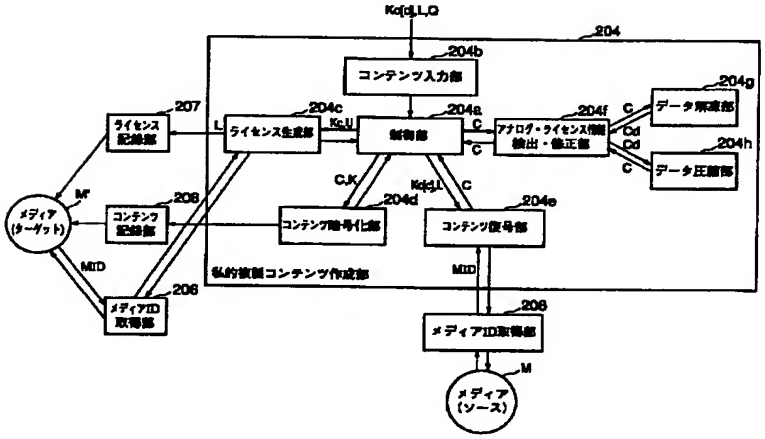
【図１９】


暗号化ライセンス復号処理
S91
暗号化デジタルライセンス情報Lを入力する
S92
デジタル署名を検証する
S93
デジタル署名は検出できたか？
NO
S101
エラー出力
YES
S94
デジタル署名検証鍵を取得する
S95
デジタル署名を検出する
S96
デジタル署名は正しいか？
NO
S102
エラー出力
YES
S97
メディアID(MID)を取得する
S98
w=f(MID)によってライセンス鍵を取得する
S99
ライセンス鍵で暗号化デジタルライセンス情報を復号する
S100
デジタルライセンス情報を出力する
END

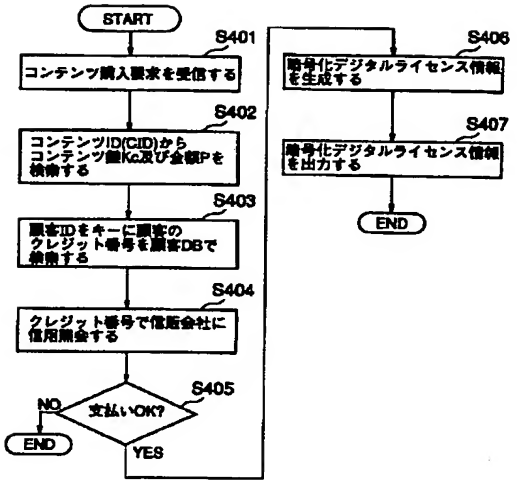
【図２１】



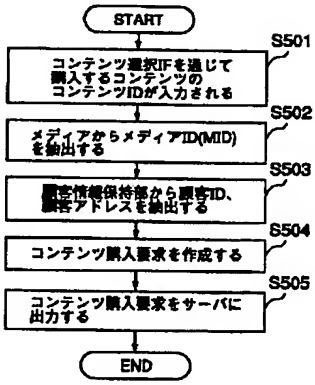
【図２２】



【図３７】



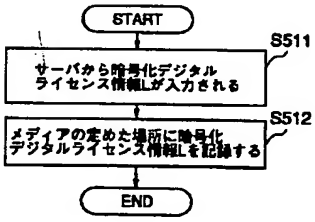
【図４１】



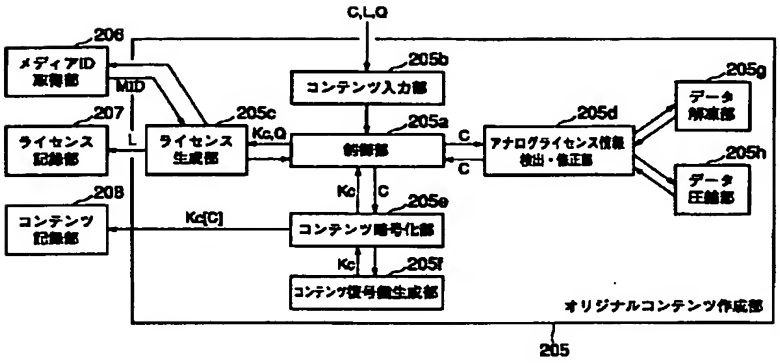
【図３９】

顧客ID	コンテンツID (CID)	購入利用条件Uc	メディアID (MID)	クライアントアドレス

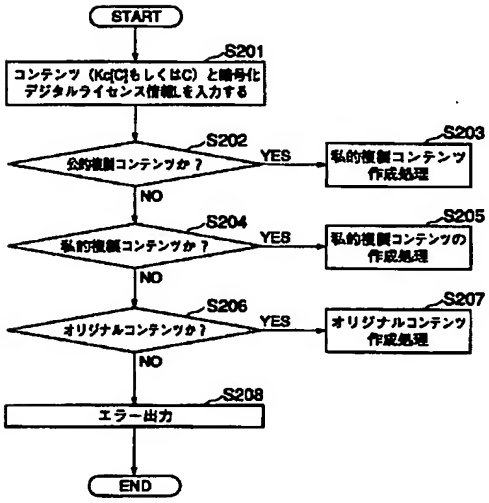
【図４２】



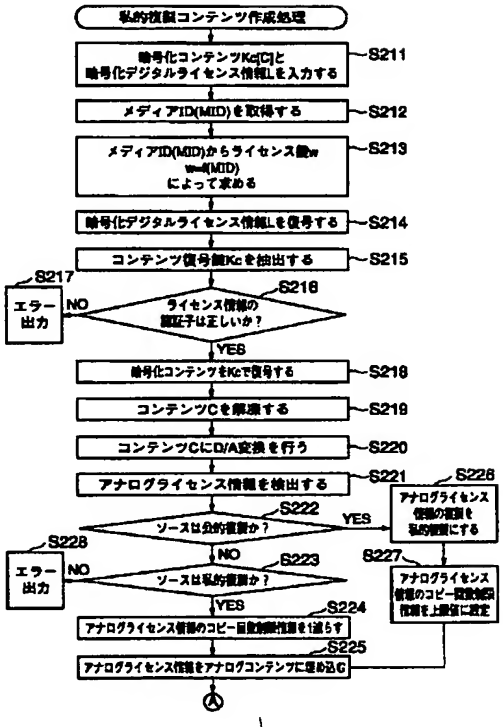
【図２３】


C,L,Q
206
メディアID
取得部
MID
205b
コンテンツ入力部
205g
データ
解凍部
207
ライセンス
記録部
L
205c
ライセンス
生成部
Kc,Q
205a
制御部
C
205d
アナログライセンス情報
検出・修正部
C
205h
データ
圧縮部
208
コンテンツ
記録部
Kc[C]
Kc
C
205e
コンテンツ暗号化部
Kc
205f
コンテンツ復号鍵生成部
オリジナルコンテンツ作成部
205

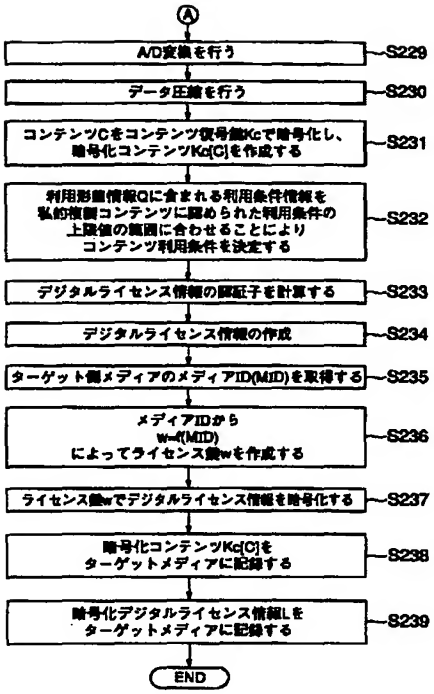
【図２４】


START
S201
コンテンツ（Kc[C]もしくはC）と暗号化
デジタルライセンス情報Lを入力する
S202
公的複製コンテンツか？
YES
S203
私的複製コンテンツ
作成処理
NO
S204
私的複製コンテンツか？
YES
S205
私的複製コンテンツの
作成処理
NO
S206
オリジナルコンテンツか？
YES
S207
オリジナルコンテンツ
作成処理
NO
S208
エラー出力
END

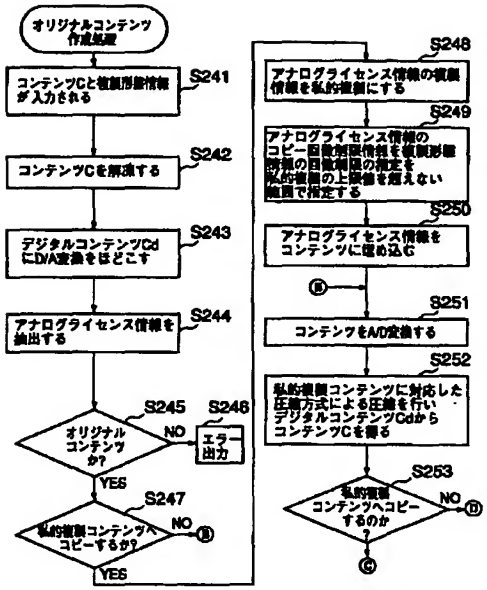
【図２５】


私的複製コンテンツ作成処理
暗号化コンテンツKc[C]と
暗号化デジタルライセンス情報Lを入力する
S211
メディアID(MID)を取得する
S212
メディアID(MID)からライセンス鍵w
w=f(MID)
によって求める
S213
暗号化デジタルライセンス情報Lを復号する
S214
コンテンツ復号鍵Kcを抽出する
S215
S217
エラー
出力
NO
ライセンス情報の
認証子は正しいか？
S216
YES
暗号化コンテンツをKcで復号する
S218
コンテンツCを解凍する
S219
コンテンツCにD/A変換を行う
S220
アナログライセンス情報を検出する
S221
S228
アナログライセンス
情報の複製を
私的複製にする
ソースは公的複製か？
S222
YES
NO
S228
エラー
出力
NO
ソースは私的複製か？
S223
S227
アナログライセンス
情報のコピー回数制御
情報を上書きに設定
YES
アナログライセンス情報のコピー回数制御情報を1減らす
S224
S225
アナログライセンス情報をアナログコンテンツに埋め込む
A

【図２６】

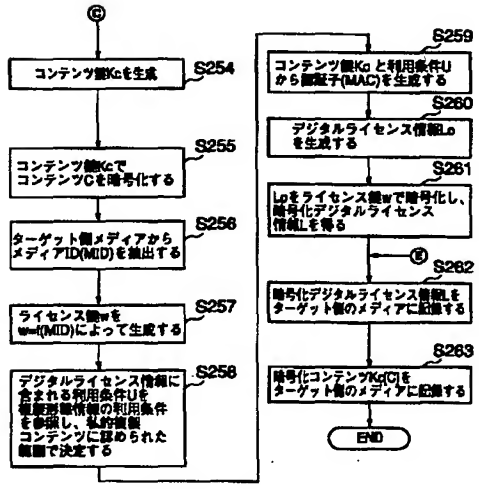


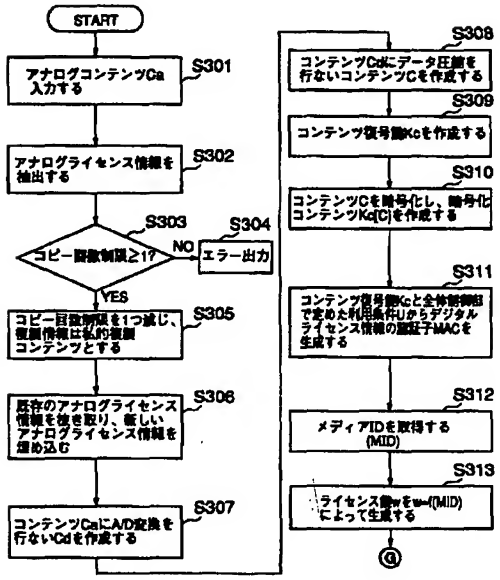
【図２７】



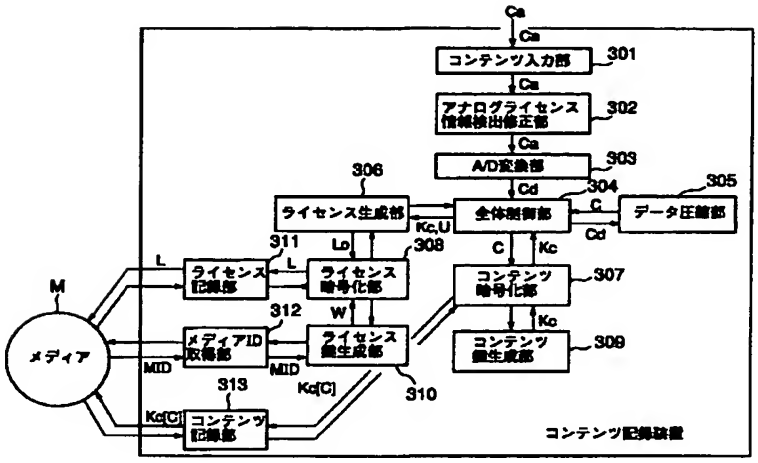
【図３３】

【図２８】

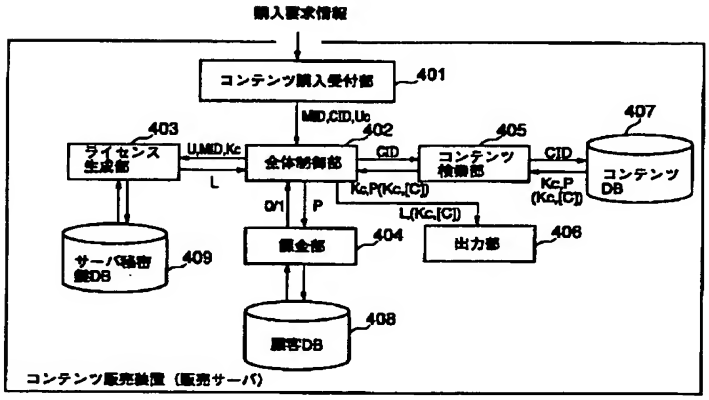




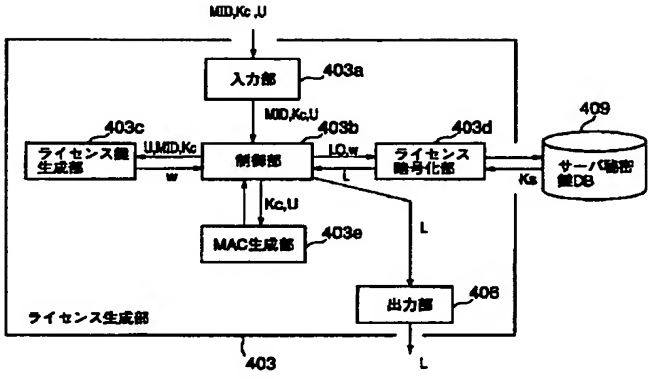
【図３２】


Ca
コンテンツ入力部
301
アナログライセンス情報検出修正部
302
A/D変換部
303
304
305
データ圧縮部
306
ライセンス生成部
全体制御部
Kc,U
C
Cd
Kc
311
Lo
308
L
ライセンス記録部
ライセンス暗号化部
コンテンツ暗号化部
307
M
メディア
312
W
メディアID取得部
ライセンス鍵生成部
コンテンツ鍵生成部
309
MID
313
Kc[C]
310
Kc[C]
コンテンツ記録部
コンテンツ記録装置

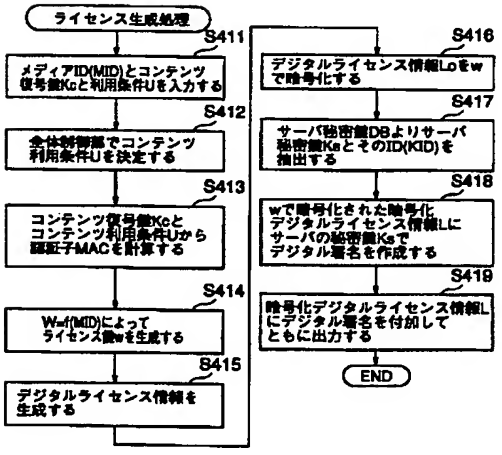
【図３５】


購入要求情報
コンテンツ購入受付部
401
MID,CID,Ub
403
402
405
407
ライセンス生成部
U,MID,Kc
全体制御部
CID
コンテンツ検索部
CID
コンテンツDB
L
Kc,P(Kc,[C])
Kc,P
(Kc,[C])
D/I
P
L(Kc,[C])
サーバ秘密鍵DB
409
課金部
404
出力部
406
顧客DB
408
コンテンツ販売装置（販売サーバ）

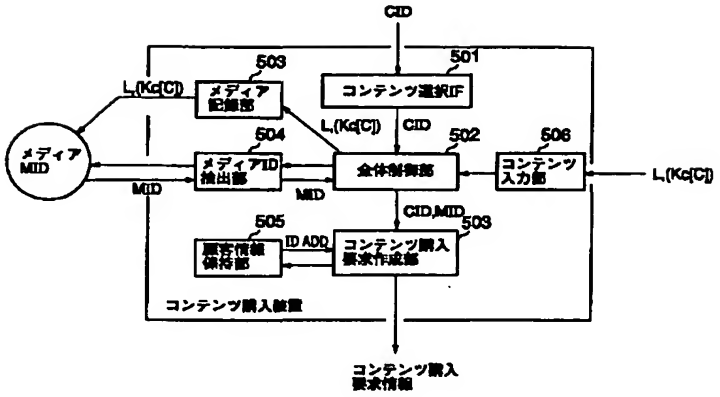
【図３６】


MID,Kc ,U
入力部
403a
MID,Kc,U
403c
403b
403d
409
ライセンス鍵生成部
U,MID,Kc
制御部
Lo,w
ライセンス暗号化部
サーバ秘密鍵DB
w
L
Ks
Kc,U
MAC生成部
403e
L
出力部
406
ライセンス生成部
403
L

【図３８】


ライセンス生成処理
S411
メディアID(MID)とコンテンツ復号鍵Kcと利用条件Uを入力する
S412
全体制御部でコンテンツ利用条件Uを決定する
S413
コンテンツ復号鍵Kcとコンテンツ利用条件Uから認証子MACを計算する
S414
W=f(MID)によってライセンス鍵wを生成する
S415
デジタルライセンス情報を生成する
S416
デジタルライセンス情報Loをwで暗号化する
S417
サーバ秘密鍵DBよりサーバ秘密鍵KsとそのID(KID)を抽出する
S418
wで暗号化された暗号化デジタルライセンス情報Lにサーバの秘密鍵Ksでデジタル署名を作成する
S419
暗号化デジタルライセンス情報Lにデジタル署名を付加してともに出力する
END

【図４０】



フロントページの続き

(72)発明者　半田　豊
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　大盛　善啓
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考)　5D044 DE17 DE48 DE49 EF05 FG18
GK12 GK17 HH15 HL07